The University of Kansas

Technical Report

Rail Sensor Testbed Program: Active Agents in Containers for Transport Chain Security

Final Report

Gary J. Minden, Victor S. Frost, Joseph B. Evans,
Jun Huan, Ruoyi Jiang, Leon S. Searl,
Dan DePardo, Ed Komp, Martin Kuehnhausen

ITTC-FY2011-TR-47750-09

January 2011

Project Sponsor:
Office of Naval Research
Contract: N00014-07-1-1042
The University of Kansas

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Rail Sensor Testbed Program:Active Agents In Containers For Transport Chain Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The University of Kansas,Lawrence,KS,66045**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The goal of this effort was to improve rail security over trade lanes, e.g., transport from Mexico to an inland port at Kansas City. This effort focused on transporter identification,sensing, real-time monitoring and tracking, safety and compliance, and integration of local, state, and federal information. We focused on transiting from the current centralized model to a distributed one. The distributed model is based on making transported objects (e.g., containers, pallets, and boxes) active agents in their own security. The effort leveraged the application of effective container sealing using advanced RFID technologies, sensing, application of new radio technologies, and information management. Evaluation prototypes were built and deployed and new distributed sensor algorithms were developed.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**60**	

Table of Contents

Section **Page**

List of Figures

Figure **Page**

Final Report
Rail Sensor Testbed Program:
Active Agents in Containers for Transport Chain Security

1 Introduction

The goal of this effort was to improve rail security over trade lanes, e.g., transport from Mexico to an inland port at Kansas City. This effort focused on transporter identification, sensing, real-time monitoring and tracking, safety and compliance, and integration of local, state, and federal information. We focused on transiting from the current centralized model to a distributed one. The distributed model is based on making transported objects (e.g., containers, pallets, and boxes) *active agents in their own security*. The effort leveraged the application of effective container sealing using advanced RFID technologies, sensing, application of new radio technologies, and information management. Evaluation prototypes were built and deployed and new distributed sensor algorithms were developed.

Section 2 outlines the approach to the project. Section 3 describes the research tasks and Section 4 lists published papers and personnel who worked on the project.

There are two appendices. Appendix A describes the algorithms used by the agents to detect anomalous events and experiments. Details and analyses of the algorithms are in the published papers. Appendix B captures "lessons learned" from our experiments and is a set of requirements for possible future systems.

2 Project Overview

Current approaches to providing security of the container transport chain are based on a hierarchical approach in terms of the collection and analysis of critical information. In all current approaches the objects being transported are passive, that is, they are simply labeled, possibly with an RFID tag (there are exceptions for some perishable items that include simple temperature sensors). The information in the label can be extensive, but is static.

The actual container transport chain, though, is governed by highly *distributed*, with complex processes, since there is no single system governing the international movement of containers. For example, the security function is distributed among industries, regulatory agencies, liability regimes and legal frameworks. Such a distributed system is not represented well by the current hierarchical approaches to security. In addition, the state of the containers being transported is *dynamic*. For example, the location, movement, temperature, means of transportation, and even access limitations of a container change from the time it is loaded until it is unloaded at its final destination.

As the cost of sensors, computing, and communications continues to decrease there is an opportunity to fundamentally change the centralized security model and move to a distributed one, which better represents the current reality. The distributed model is based

on making transported objects (e.g., containers, pallets, and boxes) *active agents in their own security*. In the distributed model each object is monitored by a set of embedded sensors and intelligent agents. An agent continuously senses its environment, the state of its object, and the state of neighboring objects. Each agent has a description of what constitutes a "secure" state. If the agent determines that the object has left the current notion of a "secure" state then a decision is required to determine whether the new state is one where the object's safety is violated or whether the change is an acceptable deviation.

As an example, consider the transport of bags of money, where each bag includes an accelerometer, a processor executing the agent program, and a radio. The bags are loaded onto a truck and the agents communicate their accelerometer readings to each other; as long as all the readings are (reasonably) consistent, the agents have a degree of confidence that they are traveling together. However, if one bag observes significantly different readings (indicating that the bag is moving in a different direction or at a different speed from the others, meaning that it is probably off the truck), then there maybe a problem which needs to be communicated (based on [2]). In this simple example the agents define a "safe" state and conditions that violate that state. The presence of two-way communications and processing provides the opportunity to enable more complex monitoring behaviors.

Our work transformed the problem from an external, periphery base model to a integrated, distributed model where agents dynamically work together and develop as a team to achieve greater security. The distributed model is that endowing physical objects with the ability to determine and communicate their sense of security through consistency of information combined with sensor observations of their environment.

The following research questions were addressed

1. How are "object security states described?" What are the semantics and ontology to describe and reason about object security states?
2. How do distributed agents form an initial mutually consistent security state? How do distributed agents maintain a mutually consistent security state?
3. How does an agent detect a change from the mutually consistent security state?
4. How does an agent determine if a detected change is permissible? How does an agent update its perspective of consistency?
5. How can trade data exchange (centralized) information be used to as part of the consistency model?
6. How does the distributed model scale (a) with number of elements, (b) with the number of objects, (c) processing time and energy, (d) communications, (e) number of sensors, and (f) number of agents?
7. What are the deployment costs and utility tradeoffs?

2.1 Rail SensorNet Architecture

In this section we describe the Rail SensorNet architecture for monitoring trusted corridors and how the distributed approach is integrated into this architecture.

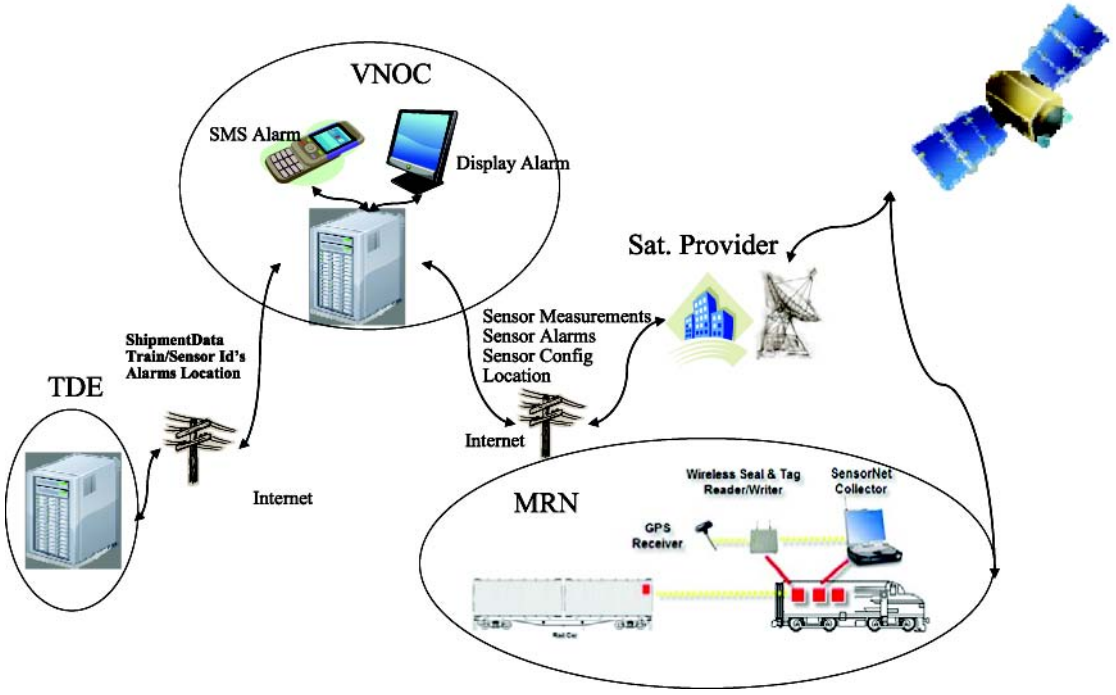

Figure 1 System Architecture of the Rail SensorNet

The Rail SensorNet is comprised of the following components:

1. A Mobile Rail Network (MRN). The MRN includes sensors on containers and cargo, a control processor in the locomotive, a GPS receiver, and one or more communications devices (e.g., cellular telephone and satellite telephone).
2. One or more communications networks, e.g., cellular telephone network, satellite network, and/or Internet.
3. A Virtual Network Operating Center (VNOC).
4. A Trade Data Exchange (TDE).

The MRN includes sensors on containers and cargo, a control processor in the locomotive, a GPS receiver, and one or more communications devices (e.g., cellular telephone and satellite telephone). The distributed agent system communications events to the MRN control processor.

The communications networks in the Rail SensorNet are commercial services. Events are transmitted from the MRN to the VNOC and control message transmitted from the VNOC to the MRN over the communications networks.

The VNOC includes a database storing data about the cargo in transit, event filtering functions, and notification services. The VNOC filters events. For example, a “Sensor Seal Open Event” when the geographical location is a known freight yard or at unexpected times or at the right time is OK. But, the same event outside the freight yard would cause an alert. Alerts are sent to responsible parties based attributes of the cargo.

An alert for a container containing hazardous material might be sent to emergency services while an alert on low value cargo might only be sent to the railroad operator. Alerts are sent via the cellular short message service, email, or Internet services.

The concept of a Trade Data Exchange is described in [4]. The TDE:

1. Captures commercial clearance data, including Shipping List, Bill of Lading, Commercial Invoice, Certificate of Origin (NAFTA Letter), and Shippers Export Declaration.
2. Interconnects commercial, regulatory and security stakeholders.
3. Validates and verifies data to ensure accuracy, consistency and completeness.
4. Performs forward notification to the customs broker to request verification of the trade origination documents. The customs broker accesses the TDE via the same portal to review and verify the trade documentation.
5. Monitors the progress of the documentation via the TDE and notifies responsible parties when errors or incompleteness pose the threat of delaying a shipment.
6. Performs risk assessment.

The applications running on the MRN, VNOC, and TDE communicate using Service Oriented Architecture (SOA) protocols. Thus, it is relatively easy to extend the system with new services.

2.2 Agent Based Systems

There are many definitions of an "intelligent agent" (or simply, "agent"), but most researchers agree that an agent is an *autonomous* program that has the ability to *sense* the environment, the ability to *communicate* with users and other agents, and the ability to *effect changes* to the environment. Additionally, agents may be able to *learn* new behaviors, *collaborate* with others to resolve conflicts or perform tasks, and *negotiate* to share limited resources.

Agent technology fits well in the proposed research since the software entities tracking the security state of a physical object, e.g., a container, need to operate continuously without human supervision (autonomously), must sense the state of the world, must be able to communicate amongst each other and possibly to other system components. In this context agents must be able to sound alarms or perform actions that change the environment. In our model agents can also learn different definitions of "security," thus expanding their knowledge. The ability to learn is essential, since it is improbable that the developers of the agents can foresee and pre-program all expected states of the world. Consequently, the agents will need the ability to expand their notion of what is a safe and what is an insecure state. Such learning requires the ability of the agents to collaborate and negotiate with others to resolve potential concerns.

Consider two example scenarios. Assume that the initial state of "safety" for a container is defined as "no change from current state." Let us also assume that the train on which a container is placed starts to move, changing the container's location and velocity. This

change in the current state would make the container agent assume it is now in a potentially unsafe state, and would lead it to query the agents around it if they thought they, too, were unsafe. A “super-agent” which has the appropriate credentials informs the container agent that the current state change is appropriate and the new state is still safe. Given that the “super-agent” has the authority to define safe and unsafe states, the container agent accepts that. The agent learns that after being loaded on a train it expects a change in location and velocity.

In the second example, the exact scenario as above is considered, but now there is no super-agent. In this case the other container agents on the train verify that they are also experiencing the same change, indicating they are all moving together. This information is compared to stored transport schedule information. If the timing of the motion is consistent with the transport schedule then the objects return to a safe state.

The approach builds upon related work on reputation systems and the web of trust approach to security. The web of trust approach (popularized by PGP in the information security community) involves the use of data (signatures) from multiple trusted sources to allow redundant verification of the veracity of the data. Reputation systems [12, 13] utilize information from multiple sources to provide a decentralized mechanism for establishing the veracity of the sources of information. These trust approaches have been applied to a variety of regimes, including virtual communities [14], email [15] and ecommerce [16] and [17], and sensor networks [18]. These approaches define trust between players and develop associated trust models; frameworks for reputation systems exist. The "sense of security" concepts we developed have similarities with trust. The paradigm requireed a technical definition of "sense of security" and development of associated models similar to [14]. Transport security requires a highly agile architecture to adapt to the inherently dynamic environment and an architecture that can embed this capability in relatively inexpensive, low-power computing and communications resources.

The new paradigm also has similarities to autonomic computing [19] where “systems manage themselves according to high-level behavioral specifications” [20]. Autonomic computing is currently targeted toward automating large computing systems like data centers. The general operation of autonomic computing involves an autonomic manager that executes a monitor-analyze-plan-execute loop that is targeted to achieve behavioral outcome, commonly system performance (e.g., maximum throughput) optimization [20].

3 Research Tasks

The research project was organized into the following tasks.

3.1.1 Model development

We identified the basic research issues associated with the proposed new paradigm. An ontology was defined, that is, the meaning of consistency and ways of establishing a mutually consistent view beteen distributed objects. An ontology is: the objects, concepts, and other entities that are assumed to exist in some area of interest and the relationships that hold among them [22]. For agent systems that are considered here, what "exists" is that which can be represented. When the knowledge of a domain is represented in a

declarative formalism, the set of objects that can be represented is called the universe of discourse. Pragmatically, an ontology defines the vocabulary with which queries and assertions are exchanged among agents. Ontological commitments are agreements to use the shared vocabulary in a coherent and consistent manner. The agents sharing a vocabulary need not share a knowledge base, each knows things the other does not, and an agent that commits to an ontology is not required to answer all queries that can be formulated in the shared vocabulary.

We defined an ontology in the context of Transport Chain Security. Distributed algorithms enabling objects to detect a change from their consistent state were developed as part of this task and are described in Appendix A. Such changes occur as the object is transported in normal situation, thus the object's perspective of consistency is dynamic.

The result of this task is the architecture for a system where physical objects are endowed with the ability to determine and communicate their sense of security through consistency of information combined with sensor observations of their environment.

3.1.2 Mapping to Enabling Technologies

In this task we mapped our distributed paradigm onto specific technologies. To test the architecture several use cases for a rail sensor testbed were developed. From these use cases one or more prototypes and experiments were designed and implemented, building upon the ongoing effort to develop SensorNet technologies to monitor trusted corridors. The result of this task is a experimental prototype design and implementation for physical objects endowed with the ability to determine and communicate their sense of security through consistency of information combined with sensor observations of their environment.

3.1.3 Prototype Development and Logistics

Testbeds and field prototypes are valuable for gaining an understanding the real-world system trade-offs and identifying practical barriers to ubiquitous use of the technology. We executed a number of experiments to collect data for testing our implementations. Results of these experiments are reported in Appendix A and published papers.

3.1.4 Prototype deployment and evaluation

We deployed prototype in the Rail SensorNet environment. Data and experiences collected during a number of trials are reported in Appendix B as a set of requirements for a future Rail SensorNet.

4 Results

4.1 Reports and Technical Papers

The following technical reports and published papers resulted from work on this project. They are available at: http://www.ittc.ku.edu/publications/index.phtml.

[1] Q. Brian, et al., "Anomaly Detection with Sensor Data for Distributed Security," in ICCCN '09: Proceedings of the 2009 Proceedings of 18th International Conference on Computer Communications and Networks, ed: IEEE Computer Society, 2009, pp. 1-6.

[2] H. Fei and J. Huan, "L2 norm regularized feature kernel regression for graph data," in Proceeding of the 18th ACM conference on Information and knowledge management, ed. Hong Kong, China: ACM, 2009, pp. 593-600.

[3] H. Fei and J. Huan, "Boosting with structure information in the functional space: an application to graph classification," in Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining, ed. Washington, DC, USA, 2010, pp. 643-652.

[4] H. Fei, et al., "GLSVM: Integrating Structured Feature Selection and Large Margin Classification," in ICDM Workshops, ed, 2009, pp. 362-367.

[5] R. Jiang, et al., "Anomaly Localization by Joint Sparse PCA and Its Implementation in Sensor Network.," in Sensor KDD, ed, 2010.

[6] B. Quanz and J. Huan, "Aligned Graph Classification with Regularized Logistic Regression," in Proc. 2009 SIAM International Conference on Data Mining, ed, 2009.

[7] B. Quanz and C. Tsatsoulis, "Determining Object Safety using a Multiagent, Collaborative System," in Environment-Mediated Coordination in Self-Organizing and Self-Adaptive Systems (ECOSOA 2008) Workshop, ed. Venice, Italy, 2008.

4.2 Personnel

The project supported the following faculty in EECS: V. Frost, G. Minden, J. Evans, J. Huan, and C. Tsatsoulis.

The project also supported Mr. Leon Searl, Mr. Dan DePardo, and Mr. Dan Deavors members of our technical staff.

The following graduate students worked on the project: R. Jiang, B. Quanz, H. Fei, M. Kuehnhausen, D. Fokum, and M. Zeets.

The following students worked on the project as undergraduates: A Oguna.

5 References

1. Kanoun, O. and H.-R. Tränkler, *Sensor technology advances and future trends.* IEEE Transactions on Instrumentation and Measurement, 2004. **53**(6): p. 1497-1501.
2. David G. Simmons. *Project Sun Small Programmable Object Technology Sun SPOTs,*. in *Based on Net-Ready Sensors: The Way Forward, Oak Ridge National Laboratory*. 2006.
3. *Container Transport Security Across Modes.* Organization for Economic Co-Operation And Development, European Conference of Ministers of Transport, 2005.
4. Dean Kothmann. *From Shelf to Shelf – Continuous Cargo Visibility and Integrity*. in *Innovation World Conference, Kansas City, Missouri*. 2006.
5. Soh, L.-K. and C. Tsatsoulis, *A Real-Time Negotiation Model and a Multi-Agent Sensor Network Implementation.* Autonomous Agents and Multi-Agent Systems, 2005. **11**(3): p. 215-271.
6. Soh, L.-K. and C. Tsatsoulis. *Utility-Based Multiagent Coalition Formation with Incomplete Information and Time Constraints*. in *IEEE International Conference on Systems, Man, and Cybernetics*. 2003.
7. Soh, L.-K. and C. Tsatsoulis, *Learning to Form Negotiation Coalitions in a Multiagent System.* AAAI Spring Symposium on Collaborative Learning Agents 2002: p. 106-12.
8. Soh, L.-K. and C. Tsatsoulis. *Reflective Negotiating Agents for Real-Time Multisensor Target Tracking*. in *Int. J. Conf. On Artificial Intelligence (IJCAI-01), Seattle, WA* 2001.
9. Soh, L.-K. and C. Tsatsoulis. *Agent-Based Argumentative Negotiations with Case-Based Reasoning* in *AAAI Fall Symposium on Negotiation Methods for Autonomous Cooperative Systems*. 2001.
10. Soh, L.-K., C. Tsatsoulis, and H. Sevay, *A Satisficing, Negotiated, and Learning Coalition Formation Architecture*, in *Distributed Sensor Networks: A Multiagent Perspective*, C. Ortiz, V. Lesser and M. Tambe Editor. 2003, Kluwer. p. 109-138.
11. Sevay, H. and C. Tsatsoulis, *Agent-Based Intelligent Information Dissemination in Dynamically Changing Environments, in: Intelligent Agents and their Applications,* in *Studies in Fuzziness and Soft Computing*, L.C. Jain, Z. Chen, and N. Ichalkaranje, Editor. 2002, Physica-Verlag. p. 1-26.
12. Resnick, P., et al., *Reputation systems.* Commun. ACM, 2000. **43**(12): p. 45-48.
13. Abdul-Rahman, A., *A framework for decentralised trust reasoning*, in *Ph.D. dissertation, University College London*. 2005.
14. Abdul-Rahman, A. and S. Hailes. *Supporting trust in virtual communities*. in *Proceedings of the 33rd Hawaii International Conference on System Sciences. Maui, HW*. 2000.
15. Boykin, P.O. and V. Roychowdhury, *Personal email networks: an effective anti-spam tool.* 2004(http://www.arxiv.org/abs/cond-mat/0402143).
16. Melnik, M., Alm, J., *Does a seller's eCommerce reputation matter? evidence from eBay auctions.* . J. Journ. of Indust. Econ., 2002. **50**(3): p. 337-349.

17. Tran, T. and R. Cohen. *Improving User Satisfaction in Agent-Based Electronic Market-places by Reputation Modeling and Adjustable Product Quality*. in *Proc. of the Third Int. Joint Conf. on Autonomous Agents and Multi Agent Systems (AAMAS-04)*. 2004.
18. Ganeriwal, S., Srivastava, M. B. . *Reputation-based framework for high integrity sensor networks*. in *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington DC, USA, October 25 - 25, 2004*. 2004.
19. Menasce, D.A. and J.O. Kephart, *Guest Editors' Introduction: Autonomic Computing.* Internet Computing, 2007. **11**(1): p. 18-21.
20. Tesauro, G., *Reinforcement Learning in Autonomic Computing: A Manifesto and Case Studies.* Internet Computing, 2007. **11**(1): p. 18-21.
21. Cybenko, G. and V. Berk, *Process Query Systems.* IEEE Computer, 2007. **40**(1): p. 62-70.
22. Genesereth, M. and N. Nilsson, *Logical Foundations of Artificial Intelligence*. . 1987, Stanford: Morgan Kaufmann.

Appendix A

Rail Sensor Tested Program: Active Agent in Containers for Transport Chain Security

Ruoyi Jiang Brian Quanz Hongliang Fei Joseph Evans Victor Frost
Gary Minden Daniel Deavours Leon Searl Daniel DePardo
Martin Kuehnhausen Daniel Fokum Matt Zeets Angela Oguna
Jun Huan
Information and Telecommunication Technology Center
University of Kansas
{jhuan}@ittc.ku.edu

January 31, 2011

Abstract

This effort focused on improving transportation security by making the objects (e.g. containers) being transported active agents in their own protection. Here, the objects are equipped with sensing and communication capabilities and are able to determine and communicate their sense of security throughout the dynamic transportation chain in a distributed manner. As part of the project, we have developed several data mining algorithms to enable intelligent agents to detect changes from their environment state. We have also designed algorithms to allow agents to communicate with each other for enhancing safety for the group of agents. Research issues of the designed algorithms have been applied to the Transportation Security SensorNet(TSSN) real transportation chain. We have tested all the new algorithms on real sensor data collected from transportation sensor network environments. The results have demonstrated the effectiveness of these algorithms for wireless sensor network security applications and provided useful insights regarding the challenges of the anomaly detection problem for distributed security in challenging environment.

Table of Contents

List of Figures

List of Tables

1. Overview

We consider the problem of fully distributed security for trade lane, and particularly when objects are equipped with sensing and communication abilities. In deriving a data-driven platform monitoring object security in transportation systems, we formalize the problem as an anomaly detection problem with data collected by wireless sensor networks. An anomaly in this report is defined as an object's observation of an event such as theft that deviates from the historical pattern or current consistent state in group of sensors. There is a wide range of applications of anomaly detection in sensor network, for instance: ensuring the safety state of buildings such as bridges [**?**], and monitoring a parking lot [**?**]. In this report, as a driving application, we work on transportation chain security. Each physical object such as container carries a computer and a wireless sensor monitoring the physical and environmental attributes of the object. Example of such attributes include the object's moving acceleration and environment temperature among others.

Different from simple signature techniques to provide security for objects, our new approaches provide a active mechanism to endow objects with the ability to determine and communicate their sense of security in a dynamic environment. We investigate several approaches for performing fully distributed anomaly detection and examine their application to the task of transportation chain security. The goal behind our approaches is to embed anomaly detection techniques in each individual sensor node to endow them with the ability to determine their own security. The algorithms used should be able to automatically learn the "normal" concept, since coming up with rules from the perspective of the particular set of sensors would be difficult if not impossible in a dynamic environment. Also, to support real-time operations the algorithms should have the capability to continuously learn and adapt while running (online), to account for concept drift present in transportation environments. Furthermore, sensor nodes typically have limited resources in terms of memory and processing power, hence algorithms that can handle resource constraints and operate in an online training fashion are preferable.

Additionally, by allowing fully distributed security, we want to utilize sharing of information between objects, for instance, sensor nodes associated with cargo in the same container in the transport chain with capabilities to communicate with each other about their observations or sense of security. In this way the objects can work together and develop as a team to achieve greater security. The security is still fully distributed since each node can make predictions of its own and send alarms. The communication ability is essential since in many cases, a change is considered as an anomaly only when it deviates from the consistency of the group. For example, a case in which all the objects in a container start to move because the container starts to move is usually an appropriate or safe situation although they are individually experiencing the change of location and velocity. Furthermore, we are able to form predictions for the network, or group, of sensor nodes by sharing opinions with nodes in the same group through communication.

Based on whether data samples are labeled or not, our approaches fall into two categories: supervised anomaly detection and unsupervised anomaly detection. In the domain of supervised anomaly detection, we focus on one class support vector machine and artificial immune systems [**?**]. We have investigated these two approaches by performing fully distributed anomaly detection and examining their application to the task of transportation chain security. After each object made a decision about its security, we considered three different ways of forming an overall group prediction in a distributed manner to achieve greater security: a baseline approach of individual detections, an event passing approach and an anomaly indication passing approach. For unsupervised anomaly detection, we considered distributed tracking

combined with Joint Space Principal Component Analysis (JSPCA) [**?**]. In short, each object uses local monitors that maintain parameterized sliding filters. These sliding filters detect local changes indicating potential unsafe states by simple threshold methods and share the changes among the objects. JSPCA uses the shared information to determine the consistent (normal) state and makes a final decision whether it is an unsafe state. In addition, at the same time as detection, JSPCA is able to identify the root object(s) where the anomaly occurred. All the approaches have been tested in the transportation security environment and experiment results have demonstrated the effectiveness of our approaches.

In addition to the general approaches and implementations of algorithms for performing anomaly detection and communication directly [**?**, **?**, **?**], we have pursued research directions addressing the challenges of applying these learning approaches to real world systems. These challenges include potentially large-scale applications (large sensor networks for monitoring large groups of objects) across various modes of transportation. Part of the challenge of making the sensor network monitoring a reality is anticipating the aspects of the data resulting from the future real-world and large-scale implementation that should be considered in constructing predictive models from and for the sensor data. In our work, we have identified several key research aspects for the real-world implementation of the distributed security sensor networks. Two of these aspects we consider are incorporating additional information about the sensor network structure (topology in the dimensions being sensed) [**?**, **?**, **?**], and addressing the dynamic nature of the sensor networks [**?**].

The work of data analysis fits into the sensor network architecture being developed by the SensorNet group at the University of Kansas. In Figure **??**, we show the system design for TSSN. Here cargo monitoring operates over a mobile rail network (MRN) which in turn communicates with a virtual network operations center (VNOC) which handles transmitting alarm events and interfacing with the trade data exchange (TDE). TDE supplies information such as shipment data. The sensor anomaly detection fits into the sensor level of the MRN, responsible for detecting events which can then be reported and handled by higher levels, aside from any local action.

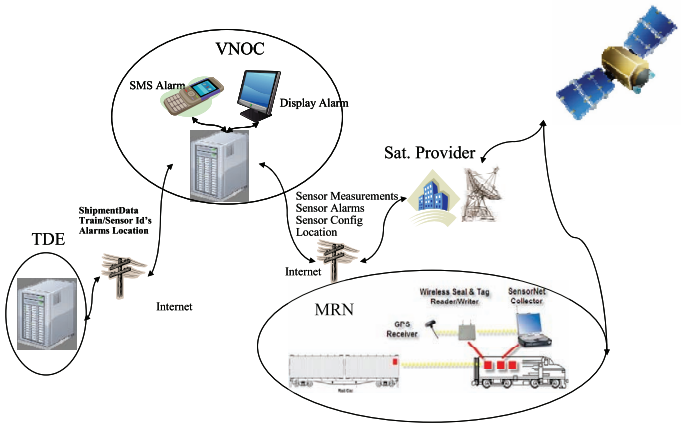

Figure 1. Transportation Security SensorNet Implementation

2. Supervised Anomaly Detection Techniques with Group prediction

The purpose of this work is to develop a detection-communication intelligent agent system. Distributed data mining algorithms are embedded into each agent to endow each one with the capability to learn its previous normal patterns and detect changes from such patterns. Once an agent detects a

change, a binary message will be broadcasted to other agents and all of the agents work as a group to make a final decision if the change should be reported or not. Different decision rules can be designed and embedded in each agent to target different events. Take the previous example, we assume that the train on which a container is placed starts to move, changing the container's location and velocity. This change in the current state would make the container agents assume it is now in a potentially unsafe state, and would lead it to broadcast their individual decision to other agents. Since all the agents are experiencing the same change and broadcast the decisions within a specified time window the agent will be reassured and no anomaly reported.

We used three base methods for distributed online anomaly detection, a resource-constrained online one-class support vector machine(OCSVM), a real-valued artificial immune system(AIS), and a simple feature threshold approach for comparison[**?**]. We extended all these three detection methods to an online setting. Then we considered three different rules of forming an overall group prediction in a distributed manner through communications that targeted different events, a baseline approach of individual detections, an event passing approach and an anomaly indication passing approach.

The OCSVM technique uses one class learning techniques for SVM and learns a region that contains the training (normal) data instances (a boundary) [**?**]. Kernels, such as radial basis function (RBF) kernel, can be used to learn complex regions. For each test instance, the basic technique determines if the test instance falls within the learned region. If a test instance falls within the learned region, it is declared as normal, otherwise it is declared as anomalous. We extended OCSVM to an online version by testing each new training instance with the current model; if it is misclassified than it is used to update the current model along with the stored training instances [**?**, **?**]. For the second base detection method, a key component of the real-valued artificial immune system (AIS) is negative selection; the goal is to define nonself (anomalies) by randomly generating a coverage of detectors around the normal, *self* region of the event space. We also have extended the real-valued negative selection to an online learning algorithm. Overall, this approach incorporates aspects of real-valued negative selection [**?**] and the online components of an AIS framework [**?**]. The third detection method is a simple threshold approach, where the max. and min. value for each feature in the training data is stored, and an anomaly is detected if a value is exceeded in the test instance.

The three approaches we used for forming the group predictions from individual detectors are individual detection method(corresponding to group OR), group event passing and group indication passing. In Group OR, no information or opinion is shared between the nodes. An anomaly is counted for the whole group whenever an individual node detects an anomaly. In effect this corresponds to an "OR" operation of the current prediction for each sensor node at a given time point. Group event passing follows a similar approach as used in [**?**]. Here when a sensor node detects an anomaly, it sends the event vector for which the anomaly was detected to its neighbors, who test the event vector with their own trained models. When a specified threshold of positive detections over the total number of predictions is reached, the event is considered an anomaly. Group indication passing focuses on anomaly events that target individual objects in the group, for instance theft of a single package. If a threshold fraction of the other nodes (we use the majority vote in our experiments) also detect a change and broadcast messages within a specified time window the node will be reassured and no anomaly reported. Thus this method focuses on anomaly events that target individual objects in the group, for instance theft of a single package.

More details about this methodology can be faced in [**?**].

2.1. Data Set

In the experiments, we tested the above algorithms on the sensor data collected for a short haul rail trial[**?**]. We used seven Sun Small Programmable Object Technology devices (or SPOTs) to collect data; six were in the box together and experimented on, and the seventh was held separately as a control to gain an idea of baseline noise. The container with the SPOTs was placed on the floor of the engine compartment, near the experimenters traveling in the engine. Periodically throughout the trip, three events were performed in sequence, a SPOT was removed from the box, about ten minutes later, returned to the box, and ten minutes after that, the box was moved. Also during one such box movement event during the trip, the box is rotated by 90 degrees, and during another, each SPOT's orientation is changed in the box. This sequence of three actions was repeated six times throughout the trip. Acceleration data from 3-axis accelerometers was used for the anomaly detection.

2.2. Experimental Results

First we obtained the results for detecting both object removal, an event effecting individual objects, and box movement, an event effecting the entire group of objects. We generated receiver operating characteristic (ROC) [**?**] curves for three anomaly detection algorithms: the resource-constrained online one-class SVM, the AIS method with a buffer, and the feature threshold method, for three group prediction approaches: individual detector ("Group OR") and two group methods ("Event Passing" and "Event Passing v2") used in concert with each base anomaly detection method. In an ROC curve the true positive rate (TPR), given as the total number of true detected anomaly events over the total number of anomaly events, is plotted against the false positive rate (FPR), which is the total number of incorrect detected anomaly events over the total number of received non-anomaly event strings from the sensor data, as a tuning parameter that trades off between these two goals is varied. The area under the curve (AUC) is usually taken as a summary of the ROC curve with a score closer to one indicating better performance of the algorithm.

Based on the experiment study, we have the following observations. First, three different detection algorithms (online one-class SVM, AIS and feature threshold) have similar performance achieving a perfect (area under curve of 1) ROC score. Second, in each figure, we found that the individual detection method (corresponding to "Group OR") was able to perform as well as group event passing methods, "Event Passing" and "Event Passing v2" (corresponding to the mean re-centering version), except for the simple feature threshold approach which had slightly less than an AUC of 1 (corresponding to 3 false positives at perfect true positive rate), but not enough of a difference to be significant. The group event passing methods, "Event Passing" and "Event Passing v2" (corresponding to the mean re-centering version), also both allowed perfect performance and were both able to correct the slight false positive rate of the feature threshold approach. In order to assess what benefit the event passing methods resulted in, we also performed an analysis of the true positive and false positive reduction. Even though ideal performance was attainable without event passing for most methods, we found event passing generally decreased the false positive rate with only slight reduction in true positive rate, and tended to increase the number of tuning parameter values for which ideal performance was obtained, thus potentially contributing to robustness. We summarize this reduction with Table **??**, showing the reductions averaged over all methods, using event passing. More details, results and analysis can be found in [**?**].

In this work, we designed a system where physical objects are able to determine their sense of security in a distributed manner and then communicate such knowledge with other objects. Final decisions of

Table 1. Averaged performance changes from using event passing

	FPR Reduction	TPR Reduction	Increase in # Perfect Scores
Avg.	0.1458	0.0287	1.3
Std. Dev.	0.2403	0.0526	1.4181

safety would be made through consistency of information combined with sensor observation of their environment. The three embedded data mining techniques we investigated can learn a local consistency from the previous data and detect changes from the historical patterns. Once a change is detected, the potential unsafe agent would share its sense of local security with other agents and then three rules are applied to examine the group consistency. Experiments on the data set collected from rail trial demonstrate the effectiveness and feasibility of the two supervised learning approaches we used. The communication between agents improve the security as well.

3. Unsupervised Anomaly Detection Techniques by Joint Sparse Principal Component Analysis (JSPCA) with Shared Information

In this section, we describe our work on a communication-detection intelligent agent system. Different from the detection-communication system in the previous section, each agent in this system determines the security of the whole environment directly based on shared observation of sensors. JSPCA anomaly detector is used to detect a global anomaly and identify the root agent of it. In order to curtail the communication cost, a local filter is embedded into each agent maintaining a local constraint. Observations will be shared and stored in each agent only if the constraint is violated in a test instance. Otherwise the previous update will be used for the further analysis to detect anomalies.

Huang [**?**] has pointed out that the detector only needs to have a good approximation of the state when an anomaly is near because the purpose is to catch anomalies deviated from consistent state, rather than to track ongoing states. He has proven that for such an approach missed detection rates remain below 4% while the data sent through the group is reduced by more than 90%. In our work, we follow his result on approximated detection and develop a JSPCA detector for anomaly detection and identification.

JSPCA detects anomalies of the whole network by the construction of a normal and abnormal subspace. Here the normal subspace is a representation of group state consistency extended by the top few principal components, while the abnormal subspace is extended by the last few principal components. All these principal components are generated by data matrix decomposition, where the data matrix is generated from the shared information gathered in a period of time. Anomalies are detected by projecting the data matrix to the abnormal subspace and comparing the projection to some threshold. If the projection is greater than some threshold, an anomaly will be reported. Since the data used is coming from all the group members, JSPCA can detect the deviation from the group consistency directly.

Additionally, JSPCA can further identify the root cause of anomalies at the same time as the detection. As the analysis in [**?**] shows, there exists a mapping between the data from each node and the corresponding entries in principal components. Such a mapping can help us to identify the node that should be responsible for the anomaly. For more details, the projection to one principal component(PC) is a summation of all the node observations weighted by corresponding entries in this PC. If one entry of one PC is zero, the corresponding node has no projection onto this direction(PC). If the entries in the same positions of all the PCs representing the abnormal subspace are zero, the corresponding node

observation can be projected to the normal subspace completely. In such situation, we can claim that this node is a normal one. Thus, our key insight of the anomaly localization is once an anomaly is detected, we check the entries across the principal components in the abnormal subspace: if the entries in the same position across the abnormal space are (close to) zero, the corresponding node is an innocent node which is not responsible for the abnormal event. However, in most situations, we cannot observe a joint zero (sparse) across the abnormal subspace, if it is directly generated from PCA. For most cases, the jth entry in one PC is close to zero, while in another PC is a large absolute value. Furthermore, the noise is expressed in the abnormal subspace as well, which causes even more difficulty in achieving simultaneous zero entries. Therefore, using PCA directly in anomaly localization is not practical in most situations. In order to overcome the challenge to get a joint sparsity in the abnormal subspace, we propose joint sparse PCA (JSPCA). JSPCA is an extension of PCA with regularization to constrain the entries in the same position of principal components to share the same sparsity pattern. Sparsity can enforces the unimportant entries to be zero or close to zero, which releases the influence of noise. Thus, the abnormal node will be located by a series of greater value across the abnormal principal components. Therefore, we can efficiently localize the anomalous node(s).

3.1. Data Set

In these experiments, the sensor data was collected during a car trial along the campus of University of Kansas. Seven Sun SPOTs were fixed in separated boxes and loaded on the back seat of a car. During the trial, each sensor recorded the magnitude of accelerations along x,y,z axis, temperature and luminance with a sample rate 3.33Hz. To collect the data for the trip, the SPOTs were programmed to continuously read and aggregate the sensor value for each sensor. We used the overall acceleration $(x^2 + y^2 + z^2)^{\frac{1}{2}}$ as the feature to detect the designed anomalous events with our anomaly detection and localization algorithm. During the whole trip, we simulated box removal and replacement, box rotation and flipping. Each event was repeated twice, in around 5 minutes interval. The whole experiment last about 1 hour.

3.2. Experimental Results

In this section, we present the anomaly detection and localization performance of JSPCA and two other benchmark algorithms Eigen Equation Compression(EEC) [**?**] and the Stochastic Nearest Neighborhood(SNN) [**?**] on the Sun SPOT sensor data collected during the car transportation trial. EEC and SNN both localize anomalies by scoring each node based on the change of neighborhood graphs. For EEC, we clustered the whole network into 3 groups for each sensor. For SNN, the neighborhood graph size k is chosen as 2. More details about these two algorithms could be faced in [**?**], [**?**]. In Figure **??**, the abnormal scores computed by JSPCA is shown in the first row of Figure **??** and the second and third rows show the anomaly scores measured by EEC [**?**] and SNN [**?**] respectively. For each algorithm, we also give the results for three different events: removal and replacement of node 2 (in the first column), flipping of node 4 (in the second column), and rotation of node 6 (in the last column). X-axis represents different nodes (seven in total)and the y-axis shows the abnormal scores, which have been normalized to the range [0,1].

Based on the experiment study, we found that JSPCA was able to localize the abnormal node accurately. As shown, we have a clear contrast between the score value of abnormal nodes(close to one) and normal nodes(close to zero). For example, in the event of node 2 removal and replacement (shown in the left figure of the top row), the abnormal score of the node 2 is significantly higher than that of the

other normal nodes. In the next two rows of Figure **??**, we show the localization performance of EEC and SNN respectively. We found that these two methods have commonality with JSPCA: all of them are able to pick out the true abnormal nodes for three events. However, EEC and SNN introduce many true positives because the score values are close to each other. Compared with these methods, our algorithm is more effective to localize abnormal objects.

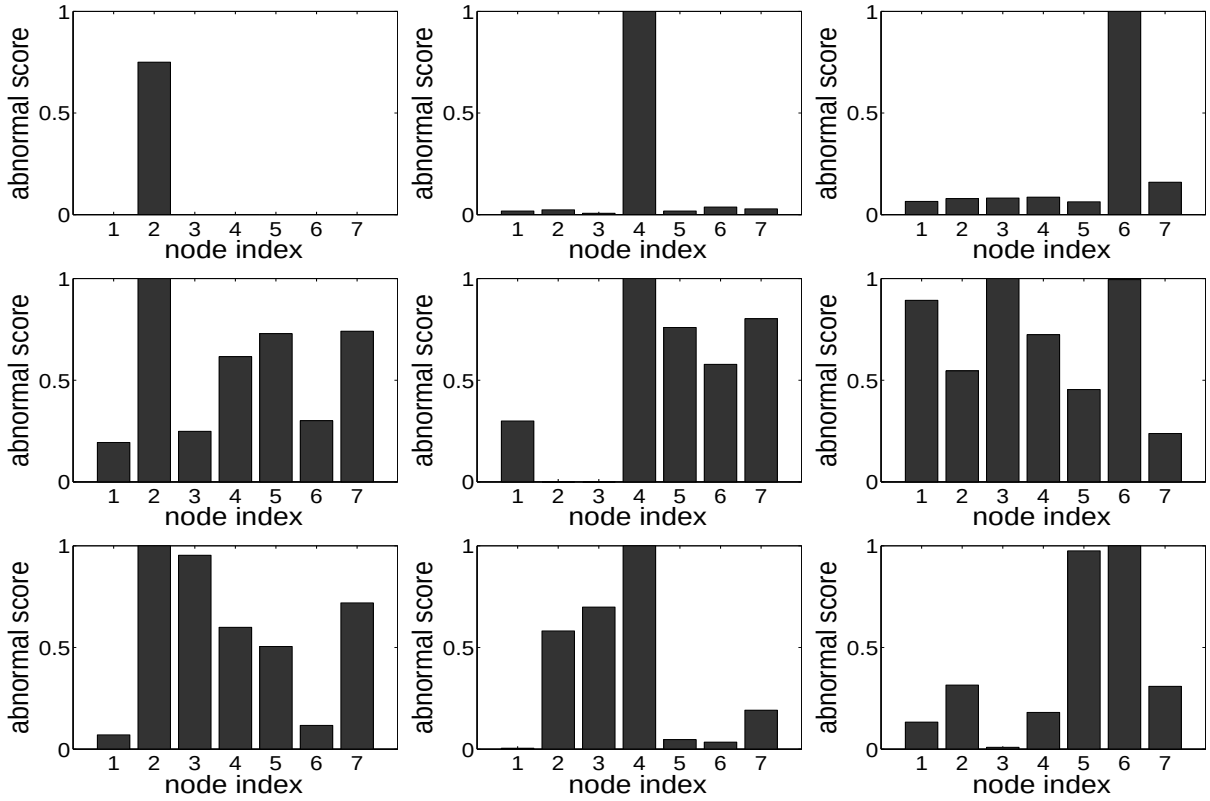

Figure 2. Comparison of JSPCA, Stochastic Nearest Neighbor and Eigen Equation Compression

We also tested this algorithm in other sensor data sets and demonstrated the stability of our method. See [**?**] for more detail.

In this work, we designed a detection algorithm JSPCA where physical objects were endowed with the ability to detect anomalies and further localize which objects have more responsibility for the detected anomalies. Different from the work in the previous section where the binary decisions(whether or not a change is detected) are made in each agent, the abnormal scores of each agent measure their contribution to a specific anomaly. Such algorithm helps us quickly localize the abnormal nodes and recover the abnormal situation.

4. Data Mining Foundation of Anomaly Detection in Wireless Sensor Networks

Aside from the above approaches and implementations directly applying to anomaly detection and localization in wireless sensor data [**?**, **?**, **?**], we have pursued research directions addressing the challenges of application of these predictive model learning approaches to real world systems, which includes potentially large-scale applications (large sensor networks for monitoring large groups of objects) across various modes of transportation. As mentioned in the overview, our investigation of the challenges of

anomaly detection consists of incorporating additional information about the sensor network structure (topology in the dimensions being sensed), and addressing the dynamic nature of the sensor networks.

4.1. Network Topology In Sensor Network Anomaly Detection

Our initial general approach to performing the anomaly detection for the sensor network data involved using classification models either globally on the sensor network or locally at each node [**?**, **?**, **?**]. However, building a model of predicted anomaly given sensed values only ignores an important source of information - the specific topological structure of the network. For example, for accelerometer data (e.g. measuring vibrations), we would expect physically nearby sensor nodes to sense similar values, for example as a person walks through an area with a senor network and walks close by a specific sensor node the accelerometer readings will be strongest in an area around where the person steps, so that nearby nodes will sense similar values; another example is temperature gradients. In general if we view our sensor network as a sensing field, sensed values will tend to vary smoothly over the field. Thus we investigated the idea that we may be able to improve the accuracy of predictive models if we incorporate this topological structure between the sensed values, or features, into the model inference process. We introduced the concept of using a feature graph, a graph between the features (corresponding to specific sensed values), that describes the topological structure of the features, and use it to bias the model learning under a regularized regression paradigm [**?**]. The idea is to use the feature graph Laplacian in a regularization term in the model optimization problem so that the model parameters vary smoothly over the feature graph. Afterward we extended the approach to the specific regression model of support vector machines as used in our general sensor network anomaly detection approach [**?**, **?**], and incorporated feature selection to identify which values are the most important for the predictive model [**?**]. Motivated from [**?**], we investigated a boosting approach [**?**], in which a set of base learners are combined to achieve a more accurate prediction. In [**?**], a boosting algorithm considering structure information among base learners was proposed. The smoothness is imposed over the similar base learners. Suppose each sensor is an agent (running an anomaly detection algorithm individually) that can provide an opinion about the current status of the network, the algorithm investigates how to combine weak decision of each sensor into a stronger one. Also, by boosting on each learner, we can identify several sensors that contribute to the anomalies. The algorithm utilizes the topology among the sensors and assigns more weights to neighboring sensors if a sensor is suspicious about an anomaly. The method can be applied to decision fusion in sensor networks for anomaly detection.

We also investigate graph based anomaly detection, which is used for determining the whole state of the network. The assumption of this method is that most of the anomalies are caused by topological changes, such as node missing, unnecessary link and anonymous node invasion. For each time stamp, we model the network topology as a graph, in which each node represents a sensor; each edge represents a relationship between two nodes. The relationship can be captured by communication signal strength or sensor reading correlation. Our preliminary experiments show that the signal strength is very sensitive to sensor orientation and spatial position, hence the signal strength is not a good way to construct graphs, especially in a noisy environment. Correlation between sensor readings is a potential approach to build graphs. In [**?**], we evaluate the graph classification problem considering the internal structure of subgraph features using an L2 norm regularized kernel matrix.

Since our own sensor network data was limited to a small network and simulated experiments on a miniaturized scale, the utility of incorporating topology is not evident at this stage, so we chiefly validated our algorithms with a number of benchmark data sets on related types of tasks that had network

structure between features. Subsequently this feature-graph regularization approach has become an emergent area of research in the data mining / machine learning communities. More details can be faced in [**?**, **?**, **?**, **?**]

4.2. Transfer Learning in Anomaly detection

Traditional machine learning/data mining approaches for learning predictive models from data rely on assumptions about near ideal data collection and generation conditions which are unrealistic for real world data such as sensor data. One typical assumption is that the collected data come from some fixed underlying distribution, i.e. that they are identically distributed. However this is generally not the case for sensor network monitoring data, in which the network itself, the environment it's in, and the nature of the monitoring tasks can be considered as dynamic entities that can change over time, and as a learned model is applied to different scenarios or specific sensor network systems. Thus we must be able to adapt learned predictive models for sensor networks to new situations as they arise, for example, as the network itself and the environment change over time, as the model is applied to different networks for potentially different but related monitoring tasks, as the normal and anomalous behavior the sensor network is monitoring changes, and as the sensor network moves between different modes of transportation. The process of transferring knowledge between data sources, e.g. from a set of collected supervised sensor data to a new monitoring situation, has been given the name transfer learning in the machine learning and data mining communities. We investigated the problem of transferring knowledge from one training data set to different test sets for which we did not yet have ground truth knowledge, i.e. the idea of adapting knowledge or a learned model from an initial training run for the distributed security sensor network to new situations and networks. We developed transfer learning algorithms based again on the regularized regression, and specifically support vector machine, paradigm [**?**]. The idea was to include a regularization term in the model learning optimization problem that would encourage the model learned to generalize across data generating distributions - essentially introducing a bias toward a solution (model) that would allow knowledge transfer. We thus used a distribution distance measure in the regularization term that was efficient to implement and could be incorporated in the kernel learning framework, where the kernel is an inner product function implicitly mapping data points to a new feature space to allow nonlinear decision functions to be learned. Again since our own current sensor data is limited in complexity and scale [**?**] we validated our algorithms using a variety of data sets including benchmarks commonly used in the machine learning/data mining literature and data sets closely related to the anomaly detection tasks with shifting data generating distributions, for example detecting spam mail.

More recently we have been investigating an algorithm-free approach to transfer learning, by learning a feature embedding, which allows us to learn a common (feature) representation for different data sources while simultaneously addressing the heterogeneity among the data sources. For example, truly heterogeneous real world data typically do not have all of the same features extracted, and missing values are still common, for example, heterogeneous sensor networks are often made up of diverse combinations of sensor nodes that may have different sets of sensors, and sensor or transmission failure is common. The approach we take is to learn a set of underlying causes that best explain the data, but also generalize across data generating distributions. More details can be faced in [**?**]

5. Conclusions and Future Work

We have investigated several approaches to perform anomaly detection algorithms with sensor data for maintaining the security of transportation chains. We have evaluated these algorithms as a proof of concept on real sensor data collected during car and rail transport trials. Experiments on the data sets have demonstrated the feasibility of our approaches.

In the future, we will continue the investigation of JSPCA algorithm and an algorithm-free approach to transfer learning. The future work of JSPCA focus on two directions. First, PCA approaches is limited to linearly correlated data and may fail to deliver optimal results when non-linear correlation exists between the sensors. Table 1 summarizes the key results obtained from our research. Second, integrating the network topology information of a sensor network to JSPCA is also a major direction in future work. As for the future work for transfer learning, by learning a feature embedding, we can learn a common (feature) representation for different data sources while simultaneously addressing the heterogeneity among the data sources. For example, truly heterogeneous real world data typically do not have all of the same features extracted, and missing values are still common, for example, heterogeneous sensor networks are often made up of diverse combinations of sensor nodes that may have different sets of sensors, and sensor or transmission failure is common. The approach we will take is to learn a set of underlying causes that best explain the data, but also generalize across data generating distributions.

Acknowledgments

This work has been partially supported by an Office of Naval Research award N00014-07-1-1042.

References

[1] *Proceedings of the SIAM International Conference on Data Mining, SDM 2009, April 30 - May 2, 2009, Sparks, Nevada, USA*. SIAM, 2009. 5, 11, 12

[2] S. G. Cheetancheri, J. M. Agosta, D. H. Dash, K. N. Levitt, J. Rowe, and E. M. Schooler. A distributed host-based worm detection system. In *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*, New York, NY, USA, 2006. ACM. 6

[3] M. Davy, F. Desobry, A. Gretton, and C. Doncarli. An online support vector machine for abnormal events detection. *Signal Processing*, 86:2009–2025, 2006. 6

[4] H. Fei and J. Huan. L2 norm regularized feature kernel regression for graph data. In *CIKM*, pages 593–600, 2009. 11, 12

[5] H. Fei and J. Huan. Boosting with structure information in functional space: an application to graph classification. In *KDD*, 2010. 5, 11, 12

[6] H. Fei, B. Quanz, and J. Huan. Glsvm: Integrating structured feature selection and large margin classification. In *ICDM Workshops*, pages 362–367, 2009. 5, 11, 12

[7] D. T. Fokum, V. S. Frost, D. DePardo, M. Kuehnhausen, A. N. Oguna, L. S. Searl, E. Komp, M. Zeets, J. B. Evans, and G. J. Minden. Experiences from a Transportation Security Sensor Network Field Trial. Technical Report ITTC-FY2009-TR-41420-11, Information Telecommunication and Technology Center, University of Kansas, Lawrence, KS, June 2009. 7

[8] S. Hirose, K. Yamanishi, T. Nakata, and R. Fujimaki. Network anomaly detection based on eigen equation compression. In *KDD '09: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1185–1194, New York, NY, USA, 2009. ACM. 9

[9] S. A. Hofmeyr and S. Forrest. Architecture for an artificial immune system. *Evolutionary Computation*, 8(4):443–473, 2000. 6

[10] L. Huang, M. I. Jordan, A. Joseph, M. Garofalakis, and N. Taft. In-network pca and anomaly detection. In *In NIPS*, pages 617–624, 2006. 8

[11] T. Idé, S. Papadimitriou, and M. Vlachos. Computing correlation anomaly scores using stochastic nearest neighbors. In *ICDM '07: Proceedings of the 2007 Seventh IEEE International Conference on Data Mining*, pages 523–528, Washington, DC, USA, 2007. IEEE Computer Society. 9

[12] Z. Ji and D. Dasgupta. Real-valued negative selection algorithm with variable-sized detectors. In *Genetic and Evolutionary Computation Conference (GECCO)*, volume 3102, pages 287–298. Springer, 2004. 6

[13] R. Jiang, H. Fei, and J. Huan. Anomaly localization by joint sparse pca and its implementation in sensor network. In *Sensor KDD*, 2010. 5, 8, 10, 11

[14] B. Quanz and J. Huan. Aligned graph classification with regularized logistic regression. In *Proc. 2009 SIAM International Conference on Data Mining*, 2009. 4, 5, 6, 7, 10, 11, 12

[15] B. Quanz and J. Huan. Large margin transductive transfer learning. In *CIKM*, pages 1327–1336, 2009. 5, 12

[16] B. Quanz and C. Tsatsoulis. Determining object safety using a multiagent, collaborative system. In *Environment-Mediated Coordination in Self-Organizing and Self-Adaptive Systems (ECOSOA 2008) Workshop*, Venice, Italy, October 2008. 5, 10, 11

[17] B. Scholkopf, J. C. Platt, J. C. Shawe-Taylor, A. J. Smola, and R. C. Williamson. Estimating the support of a high-dimensional distribution. *Neural Computation*, 13(7):1443–1471, 2001. 6

[18] H. Song, S. Zhu, and G. Cao. Svats: A sensor-network-based vehicle anti-theft system. In *INFOCOM*, pages 2128–2136, 2008. 4

[19] N. Xu, S. Rangwala, and et al. A wireless sensor network for structural monitoring. In *IN SENSYS*, pages 13–24, 2004. 4

[20] Z. Zhang and H. Shen. Application of online-training svms for real-time intrusion detection with different considerations. *Computer Communications*, 28:1428–1442, 2005. 6

Appendices

A. Published Papers

Key Results	Title	Author	Publisher	Appendix
A framework consisting of agents with case-bases of threat detection systems and a mechanism for sharing and confirming beliefs with other agents are proposed.	Anomaly Detection with Sensor Data for Distributed Security	Brian Quanz, Hongliang Fei, Jun Huan etc.	in Proc. Environment-Mediated Coordination in Self-Organizing and Self-Adaptive Systems (ECOSOA 2008)	A.1
Two algorithms OCSVM and AIS are investigated to perform fully distributed anomaly detection. Communication between sensors is utilized to enhance group safety.	Determining Object Safety using a Multi-Agent Collaborative System	Brian Quanz, Costas Tsatsoulis	in Proc. 2nd Int'l Workshop on Sensor Networks (SN 2009)	A.2
Develop distributed JSPCA, which is able to define the group consistency, detect change from such consistency and identify the root cause of the change.	Anomaly Localization by Joint Sparse PCA in Wireless Sensor Network	Ruoyi Jiang, Hongliang Fei and Jun Huan	in Proc. 4th International Workshop on Knowledge Discovery from Sensor Data (SensorKDD-2010)	A.3
Transfer learning is investigated to address the dynamic nature of sensor network	Large Margin Transductive Transfer Learning	Brian Quanz, Jun Huan	in Proc. 18th ACM Conf. Information and Knowledge Management (CIKM'09)	A.4
Network topology in sensor network is investigated to better define consistency of state.	Boosting with Structure Information in the Functional Space: an Application to Graph Classification	Hongliang Fei and Jun Huan	in Proc. the 16th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (SIGKDD'10)	A.5
Network topology in sensor network is investigated to better define consistency of state	L2 Norm Regularized Feature Kernel Regression For Graph Data	Hongliang Fei and Jun Huan	in Proc. the 18th ACM Conf. Information and Knowledge Management (CIKM'09)	A.6
Network topology in sensor network is investigated to better define consistency of state	GLSVM: Integrating Structured Feature Selection and Large Margin Classification	Hongliang Fei and Jun Huan	in Proc. Workshop on Optimization Based Methods for Emerging Data Mining Problems (OEDM 2009)	A.7

Network topology in sensor network is investigated to better define consistency of state	Aligned Graph Classification with Regularized Logistic Regression	Brian Quanz and Jun Huan	in Proc. the SIAM Data Mining Conference (SDM 2009)	A.8

Appendix B

SensorNetIII Requirements Document:

Container Transportation Security Network

Leon S. Searl, Ed Komp, Dan DePardo, Dan Deavours and Martin Kuehnhausen

2011, January 24

1 Introduction

Contained in this document are the Requirements for SensorNetIII. SensorNetIII is the follow on project of SensorNetI(Transportation Security SensorNet) and SensorNetII using the lessons learned from these previous projects. Container Transportation Security Network (CTSN) is the more descriptive name given to SensorNetIII. The project is specific to monitoring the security, safety and status of ISO Intermodal Containers shipped on rail and truck and sorted in sea port and rail sorting yards.

The requirements, rather than being formal, are a mix of requirements, topics that required further study and actions needed develop the remaining requirements.

Although the sea going ship segment of an Intermodal Container's journey is not considered in this document many of the requirements would be applicable and could be implemented.

2 Requirements

The sub-sections within this section contain the specific requirements, options and commentary for the Container Transportation Security Network.

In some instances the current technical knowledge base or regulatory environment prevents specific requirement generation. In these instances further technical studies or regulatory enhancement will be required.

2.1 Network Requirements

This section contains the requirements for the various components of the network. The network components are based on the network components developed for SensorNetI Transportation Security Sensor Network (TSSN).

The requirements are for messages between the Trade Data Exchange and Shipper's Network Operations Center (NOC) and between the Shipper's NOC and the Container Nodes. Between the NOC and Container nodes are Access Points and Wireless Message Relays.

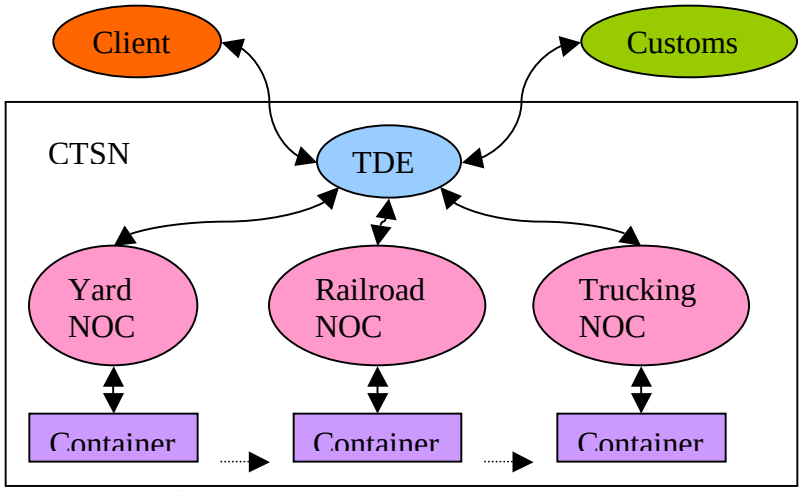

Figure 1 CTSN Player's Connectivity

Figure 1 shows the connectivity requirements of the players in a Container Transportation Security Network (CTSN). A Client/Broker communicates with a Trade Data Exchange (TDE) to setup a cargo shipment that houses the cargo in a CTSN container. The TDE communicates with the Yard (example: Sea Port Sorting Yard), Railroad and Truck shipping companies to arrange a schedule for the shipment and to hand-off custody of the shipment as it passes between the Shippers. At a customs point a customs official communicates with the TDE to obtain the container manifest and to request that security monitoring of the container be relaxed so that cargo may be inspected without setting off alarms. The Shippers communicate with the containers during transit to monitor security and health of the container and report security issues concerning the container to the TDE. The TDE reports container issues to the client when necessary.

2.1.1 TDE and Shipper NOC Network Requirements

Messages between the TDE and NOCs are used in the scheduling and custody exchange of containers between Shippers. These messages are also used for checking and reporting the status of cargo shipments.

The concept of the Trade Data Exchange is a carry over from SensorNetII. For the purposes of this requirements document, the TDE is the portal for shipping clients and customs officials to interface to the CTSN. It also coordinates the transfer of custody of containers from one Shipper to another ensuring that there is always a Shipper taking responsibility for a container during its journey. The TDE is the only authority allowed to make security related configuration changes to the node on a CTSN container.

Each Shipper has a NOC that is responsible for communicating with the TDE and the Container Nodes in the Shipper's custody. Container Node security is monitored and any issues are reported to the TDE.

Requirements of communication between the TDE and NOCs not included in this version of the document include:

- General authentication and authorization
- General message confidentiality/privacy
- Subscription and publication of events/notifications
- Service discovery
- Communication architecture (SOA, ROA, etc).

The following requirements of this section are largely derived from the SensorNetII project.

R-2.1.1.1.1 Each Shipper in the CTSN shall have one or more Unique IDs that identify the Shipper in network messages.

The Shipper Unique ID is used to identify Shippers in network messages. A Shipper may have more than one ID to identify different regions of the globe that the Shipper operates in or different subsidiaries of the Shipper. Each Shipper Unique ID is associated with a unique NOC.

R-2.1.1.1.2 All network messages between CTSN Shippers shall be digitally signed to provide high confidence that the message has not been altered during its travel from the source to the destination.

The digital signing method for messages at this level of the network needs further study and must be agreed upon by a consortium of participants. Since these messages traverse high speed networks with virtually unlimited processor power available the signature length may be long and more computationally intensive compared to the signatures of messages in the Container Network.

R-2.1.1.1.3 The TDE shall provide a Shipper with a best estimate container pickup time and location with sufficient advance notice to prepare for the pickup.

As an example, when a ship carrying containers is to arrive at a sea port sorting yard, the sorting yard must have sufficient time to prepare an empty storing area within the yard for the containers.

For rail transport from a sea port rail yard, the railroad company must move a sufficient number of rail well cars to the rail yard for the expected number of containers.

To transport a container by truck from a sorting yard, the trucking company must send a truck to the sorting yard at the appropriate time.

The same pickup time message is used to notify the Recipient Shipper when a pickup time has changed.

R-2.1.1.1.4 A Shipper shall notify the TDE of a container it is picking up (accepted) from the container's route source or the previous Shipper in the shipping chain.

This requirement is part of the chain of custody requirements. A Shipper that has accepted a container is the Custodian Shipper of the shipment.

The actual pick-up time is included in the messages.

The TDE uses the Custodian Shipper's network to notify the Container Node of the new custodian.

R-2.1.1.1.5 The TDE shall have the capability to query the container's Custodian Shipper for the estimated drop-off time of the container based on current movement state of the container.

Using current location, speed and anticipated speed, current and forecast weather conditions and handling time the shipper will estimate the drop-off time of the container.

R-2.1.1.1.6 The TDE shall have the capability to query a Shipper that is in the shipping chain of the container, but has yet to have custody of the container, for the estimated drop-off time of the container based on current estimated pick-up time.

Using estimated pickup time, forecast weather, transportation time and handling time the Shipper shall return the estimated drop-off time.

R-2.1.1.1.7 When the Custodian Shipper has determined that an estimated delivery time has changed due to weather, mechanical failure, human error or other unanticipated events, the Custodian Shipper shall notify the TDE of a new estimated drop-off time.

The TDE shall use the new estimated drop-off time to notify the remaining Shippers in the container's shipping chain of the new estimated pick-up time and ask for a new estimated drop-off time.

R-2.1.1.1.8 A Shipper shall notify the TDE of delivery at its final destination or the transfer of custody to the next Shipper in the shipping chain.

This requirement releases a Shipper from custodianship of the container if the container is being delivered to its destination or as soon as custody is accepted by the next Shipper.

The actual delivery time is included in the message.

This message to the TDE must occur before the next Custodian Shipper can be assigned to the Container Node.

R-2.1.1.1.9 A Cargo Vendor/Recipient shall have the capability to query the TDE for the location of a container.

The TDE queries the Custodian Shipper for the location of the Container Node. The location resolution is not required to be finer than the RF coverage area of the Access Point the Container Node is within. If a finer resolution location is available (Container Node GPS, location determination using RF signal strength and direction, container stack Coupled Magnetic Field location, etc.) then the finer resolution location is used.

The location response shall contain at least the following location information:

- Latitude and Longitude of last location update
- Time stamp of last location update
- Confidence in the location:
  - Good
  - Estimated
  - Location Unknown – Location Unknown generally means that that communication with the Container Node been lost.

R-2.1.1.1.10 A Shipment Client may query the TDE for cargo sensor values. This message may be encrypted.

See the TDE-Shipper Cargo Sensor query requirement for more in formation.

R-2.1.1.1.11 The TDE may query a Shipper for the location of a container. This message may be encrypted.

See the Client-TDE Location Query requirement for the shipment client view of this request.

If the Container Node is equipped with GPS the Container Node GPS position is reported, otherwise the Shipper may report the position of the Access Point communicating with the Container Node.

A rail Shipper may use a more involved method of estimating location. If the rail Shipper knows the rail car position of the container in a train, the Container Node location may be estimated based on the Access Point GPS position and the rail car position in the train.

In a sorting yard, the location of each container is known by yard row and section, allowing latitude and longitude coordinates to be calculated without the need for GPS, although the GPS position of the Access Point communicating with the container should be used to provide a validity bound for the calculated container location.

R-2.1.1.1.12 The TDE may query a Shipper for cargo sensor values. This message may be encrypted.

Cargo within a container may have its own sensors that can be queried by the Container Node. This requirement allows the CTSN network to be used by a client to query the cargo sensors.

The cargo sensor query and the values returned by the cargo sensors may be confidential. To provide confidentiality the query and response messages may be encrypted.

The cargo sensors must comply with the wireless sensor specification that results from another requirement in this document concerning communication between cargo sensors and the Container Node.

R-2.1.1.1.13 A Shipper shall notify the TDE of any Container Node generated Alarm messages.

The TDE logs all Alarm messages from the Container Node and notifies the Shipment Client.

The method of client notification is not specified in this document.

R-2.1.1.1.14 The TDE may query the current Container Node's custodian shipper for the Container Node's event Log.

When there is an Alarm message from the Container Node, reviewing any preceding Warning or Info events may help resolve the cause of the Alarm.

Warnings and Info events are usually of no value at the TDE level so they are not reported to the TDE unless requested by the TDE.

R-2.1.1.1.15 The TDE may command the Custodian Shipper of a Container Node to clear the Node's event log.

This requirement is intended to be used at the end of a shipment when the log is no longer needed or at the beginning of the shipment if the log had not been previously cleared.

Only the TDE may request that a Container Node log be cleared. It is undesirable for a Shipper to be allowed to clear a log since the Shipper may try to avoid responsibility for

cargo theft or damage that occurred while it was custodian by clearing the Container Node log.

2.1.2 Shipper Intra Network Requirements

There are few requirements for network messaging within a Shipper's Network. The Shipper is free to use any networking medium within the NOC and between the NOC and its Access Points that meet the following requirements.

R-2.1.2.1.1 Messages between TDE and a Container Node shall pass between the Custodian Shipper's NOC and Access Points without modification.

The message between the TDE and Container Nodes may be encapsulated in the data portion of a Shipper's network message.

Shipper encryption of the messages for transfer between the NOC and Access Points with subsequent decryption of the Shipper's own encryption shall not be considered modification of the message.

R-2.1.2.1.2 The time from receipt of a TDE message at a Shipper's external network portal to the receipt of the message at the Container Node shall not exceed X seconds.

A study must be conducted to determine a number for X. X will be less than the time for determining that a Container Node is missing.

In the event that the Container Node a message destined for is missing, the NOC shall report the Container Node as missing.

In the event that an expected communication loss with the Container Node is occurring, the NOC shall report to the TDE the expected time that communication with the Container Node shall resume. Expected loss of communication may occur in remote areas where land mobile communication is used between the Access Point and the NOC but the Access Point is outside the range of the nearest communication tower.

2.1.3 Container Network Requirements

This section contains requirements pertaining to the operation and networking of communications between a Shipper's Access Point and Container Nodes. The Container Network is a wireless network of Access Points, Wireless Message Routers and Container Nodes.

These requirements consider 3 types of Container Networks.

1) Sorting Yard – The Sorting Yards are large areas to temporarily hold and sort containers when the containers are to change Shippers or change shipping conveyance. An example of a Sorting Yard is a sea side dock where containers are moved to/from ships from/to trains or trucks. As a point of reference, Sorting yards may have more than 10 thousands containers in the yard at one time.
2) Train – Containers are transported on rail using container well cars. It is not unusual for these trains to be up to 300 cars long with up to 3 containers per car.

3) Truck – Containers are transported in single units by truck over roadways.

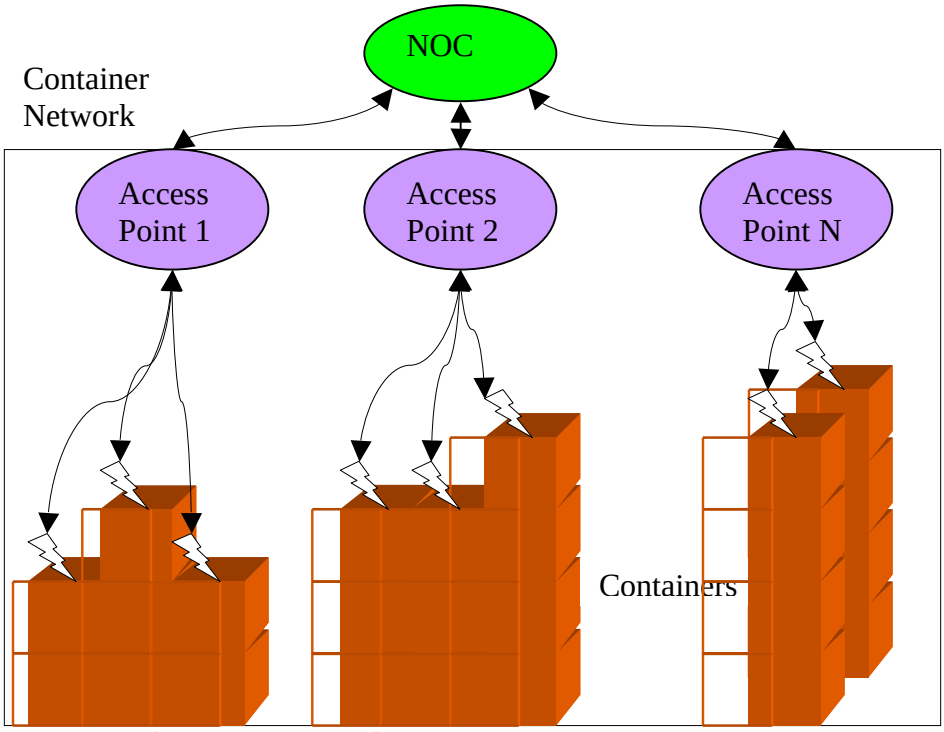

Figure 2 Sorting Yard Container Network

The diagram in Figure 2 illustrates a portion of a Container Network for a Sorting Yard. The Shipper's NOC has a connection to each Access Point in the Sorting Yard. The NOC-AP connection may be wireless or wired. This document does not specify the physical medium for the NOC-AP link. Access Points are spread through out the yard to provide RF coverage for all container locations. Access Points communicate with Container Nodes through either a RF link or a Coupled Magnetic Field.

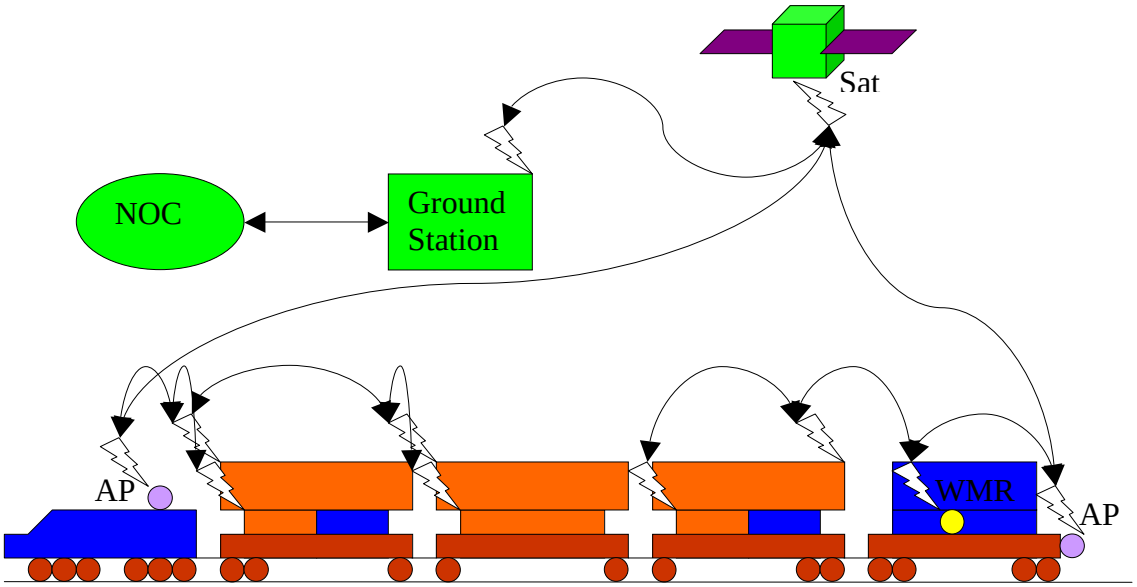

Figure 3 Train Container Network

The diagram in Figure 3 shows a schematic of a Container Network on a train. The train has two Access Points (APs). One Access Point is at the front of the train with the engine. The second is as the end of the train with the End-of-Train device. Container Nodes in the first half of the train form a wireless network with the Access Point in the engine. Container Nodes in the last half of the train form a wireless network with the trailing Access Point. Wireless Message Relays (WMR) may be used to relay messages between CTSN containers and between containers and Access Points. The WMR is particularly useful when non CTSN containers are in the train making the span between CTSN containers too great to complete a wireless connection. Since WMRs are required to have more power available than Container Nodes, they relieve the Container Nodes of the communications power consumption that would otherwise be required to relay messages to Containers Nodes out of Access Point range.

The train's APs must use a wireless communications link to the NOC. The communications link may be any number of available services including: Satellite (Iridium), Cellular (GSM, EV-DO) and Private Land Mobile (Radio).

Figure 3 illustrates one method of connecting the Shipper's NOC to the train's APs. A satellite forms a connection between a ground station and the train Access Points. The Shipper's NOC has a hard line connection to the ground station.

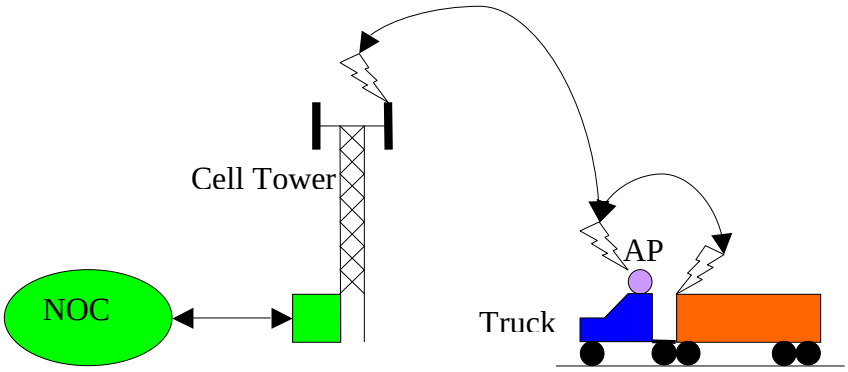

Figure 4 Truck Container Network

In Figure 4 a Truck Container Network is shown with a truck hauling a CTSN container. The Container Node communicates with the truck mounted Access Point. The Access Point uses a wireless link to the NOC, in this case through a Cellular connection.

R-2.1.3.1.1 RF Frequency use by the Container Network shall be centered at X MHz.

At this time there is no specific RF frequency requirement. The following will have to be done to have a feasible requirement:

- Determine the frequency range that is most conducive to container wireless communications in the Sorting Yard and Train configurations. Frequency selection would be based upon available spectrum and propagation simulations followed by empirical verification of the highly reflective RF environment created by stacks and lines of metal containers.
- Obtain international agreement on an unlicensed frequency range for container wireless network use.

Current unlicensed frequency ranges are not suitable for wireless container networks.

- The 435MHz ISM band is expected to be too narrow for the data rates that will be required for Container Nodes and Wireless Message Relays near the ends of trains since all of the messages from half of the containers must pass through the last relay or last few nodes nearest the Access Point in the corresponding portion of the train.
- The 2.4GHz band is heavily utilized by a range of 802.11, ZigBee, Bluetooth, and other devices which would pose interference and desensitization issues.
- The 915MHz ISM band is only available in North and South America. In addition, railroads use 915MHz readers at the trackside which can block other RF communications in the same band.
- 868MHz is only available in Europe.
- Use of unlicensed spectrum above 2.4GHz would potentially require additional power consumption by Container Nodes to offset propagation losses.

R-2.1.3.1.2 All wireless messages between CTSN containers and between a CTSN container and a CTSN Access Point shall have digitally signed messages.

This requirement is to provide high confidence that messages have not been altered during travel from the source to the destination. It also provides verification of the identity of the source of the message.

This requirement is critical for messages that are used to change the state or configuration of a Container Node. Only authorized sources (primarily the TDE) may change the configuration a Container Node.

2.1.3.2 Containers

R-2.1.3.2.1 Each CTSN container shall have an ID that uniquely identifies the container.

This ID is called the Container CTSN ID. In this document the term Container ID may also be used when there will be no confusion with any other type of container identification.

R-2.1.3.2.2 CTSN enabled containers shall be wireless networked with each other and/or with CTSN Access Points in the following shipping situations:

- Rail Transport
- Sorting yards (Railroad and Shipping)
- Over the Road Truck Transport.

We are leaving ships out of the requirements at this point since ships are reasonably secure while as sea. There is no reason that ships could not also adhere to the requirements for trains.

R-2.1.3.2.3 CTSN containers shall have two physical communications mediums.

- Coupled Magnetic Field
- RF

The various environments that intermodal containers are placed prompt the need for a hybrid communications mechanism.

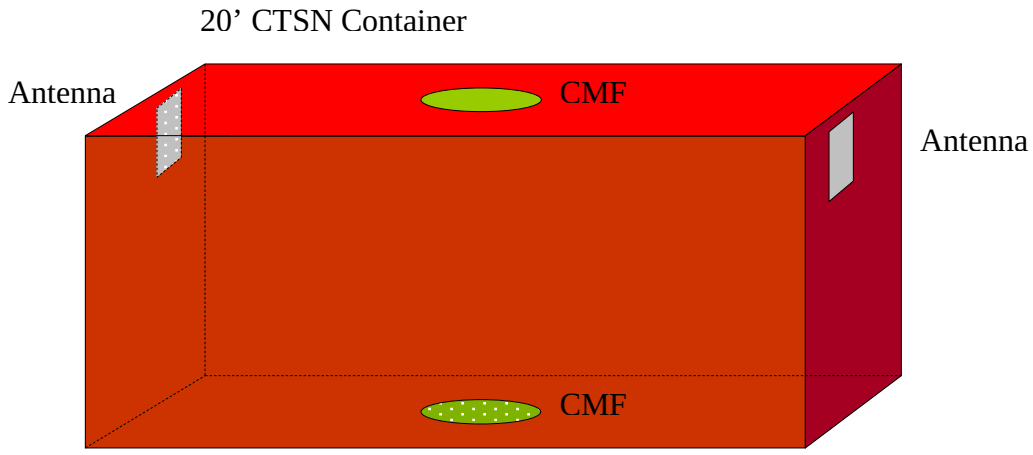

Figure 5 20' CTSN Container with RF Antennas and Couple Magnetic Field positions

When there is space around one of the Container Node’s RF antennas that is much greater than the communication frequency wavelength, using RF communications will be effective if the Container Node is within the range of an Access Point. RF communication will be used for truck transported Container Nodes and will typically be available for use on rail well cars.

When a container is tightly packed with other containers (as is the case in sorting yards) RF communication for those containers buried inside a stack may not be effective. In this case a Coupled Magnetic Field for communications between adjacent containers would be used. Messages would be relayed from a Container Node inside of a stack and to a container located where RF communication is possible.

R-2.1.3.2.4 Containers shall communicate with vertically adjacent CTSN containers by means of a Coupled Magnetic Field.

The same magnetic field coupler that serves to transfer power between containers is also used for adjacent container communications. At least one coupler is on top of the container and an additional coupler(s) is on the bottom of the container.

The couplers must be placed to align when containers are stacked.

A study must be conducted to determine the best location for the Coupled Magnetic Field coils. In particular the case of a 40 foot or longer container placed on two 20 foot containers on a rail well car must be considered.

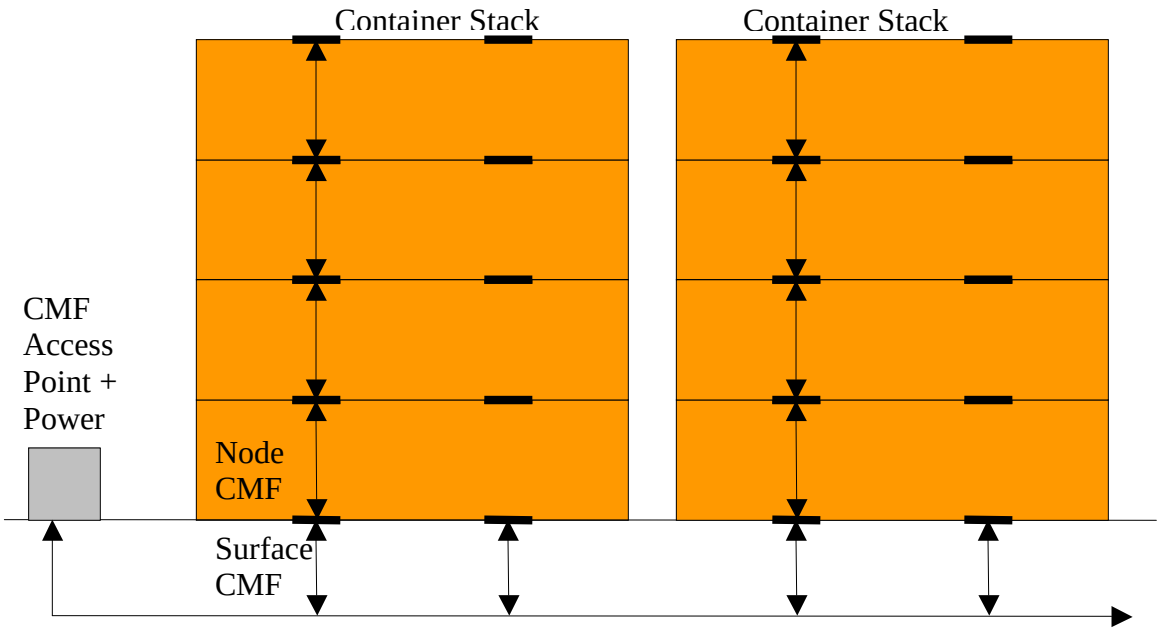

Figure 6 Sorting Yard Couple Magnetic Field Power and Communication with Nodes

R-2.1.3.2.5 Containers shall have a RF antenna mounted on each end of the container near the top of the container. The antenna and mount shall be designed such that damage to the antenna is unlikely under 'normal' container handling conditions.

An antenna mounted on the top, bottom or sides of the container would be blocked when buried in a container stack in a sorting yard making these locations unsuitable for antennas with just a few exceptions.

Since it is unlikely that all containers will be fitted with CTSN, it is assumed that there a probability of a mix of CTSN and non-CTSN containers in the same sorting yard stack. This means that some Containers Node's in a stack could be prevented from using the Coupled Magnetic Field system to communicate, due to vertically adjacent non-CTSN containers. An isolated Container Node. An isolated Container Node in a stack could potentially send and receive messages to other RF containers in the stack or an adjacent stack by way of a reflected RF signal using the antennas located at the ends of containers.

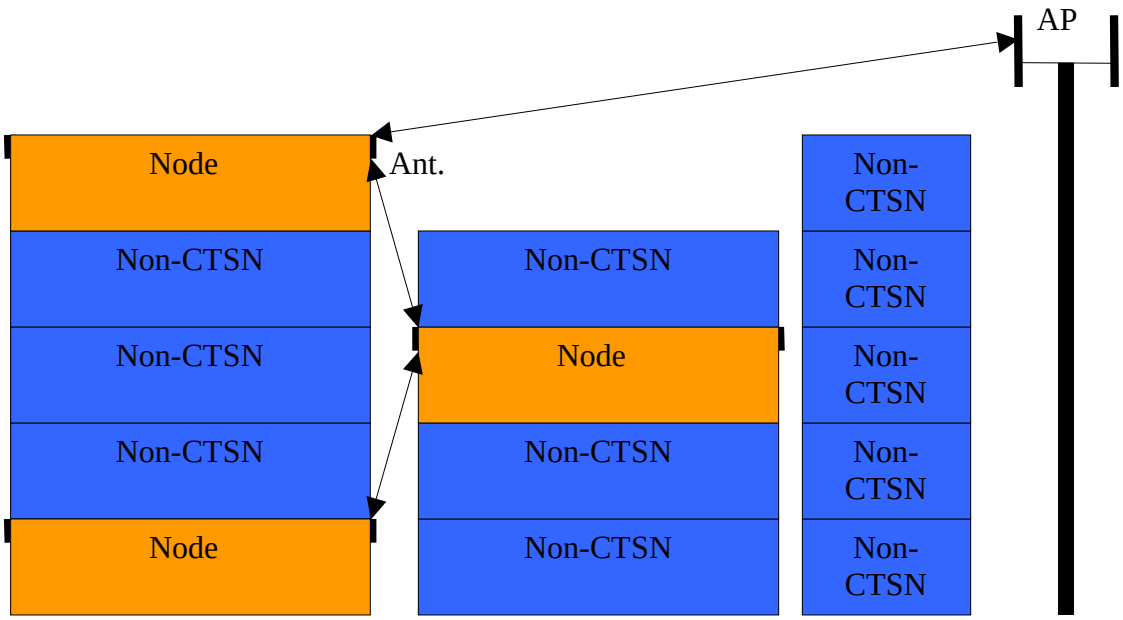

Figure 7 Container Stack with Nodes Relaying RF messages to Access Point

The only situations where antennas on the ends of containers are completely blocked are when two 20 foot containers are placed end-to-end in a rail well car. The antennas on the adjacent container ends are blocked but the antennas on the other ends of the Container Nodes are not blocked.

R-2.1.3.2.6 Container Nodes shall be network configurable to facilitate multi-hop messaging using other Container Nodes for intermediate hops.

This requirement is needed for utilizing the Coupled Magnetic Fields within a container stack, for using RF communications in a stack of sparsely populated CTSN capable containers and for train networking when there is a lack of Wireless Message Relays.

Examples of multi-hop message relaying are shown in Figure 3 and Figure 7.

R-2.1.3.2.7 Container Network topology shall be configured by a Shipper's NOC via commands sent to Access Points, Wireless Message Relays and Container Nodes.

The Shipper NOC has knowledge of the container IDs and at least general container location. This knowledge allows the Shipper NOC to determine a network configuration faster and with less Container Node power usage than an ad-hoc network determined by the container nodes themselves.

2.1.3.3 Access Points

An Access Point is a bridge between the Container Node's wireless link and the remainder of a Shipper's network. It may bridge directly to a wired network or it may use another wireless technology (802.11, GSM and other high speed digital WAN [3G, 4G, etc], Satellite Data link) to communicate with a Shipper's wired network.

R-2.1.3.3.1 All container transporting vehicles and vessels shall have at least one Access Point

- Truck – Shall have one Access Point. This access point will obtain power from the truck's electrical system.
- Train – Shall have two Access Points.
    - Shall have an Access Point located at the front of the train powered by the engine's power supply.
    - Shall have an Access Point located at the rear of the train. This requirement provides an available redundant path for Container Node data, reduces by half the amount of message traffic that must be relayed to the front Access Point when not used as a redundant data route, and can use a convenient power source in the End of Train device. The End of Train uses the compressed air from the train braking system to spin an air turbine electric generator.

R-2.1.3.3.2 Sorting Yards shall have Access Points placed in a physical topology to allow any potential CTSN container position within the yard to be within direct line range of at least one Access Point.

Direct line range assumes that no other containers are blocking the RF path between the container and the AP. In practice, many Container Nodes will not have a clear Line of Sight (LOS) path to an Access Point due to the configuration of stacked containers in a yard. This requirement is intended to set a maximum distance between CTSN Container Nodes and the nearest Access Point.

Light poles in sorting yards are potentially ideal locations to place Access Points. The light fixtures are already supplied with power and are positioned above the highest container stacks. The layout of the lights poled to provide task and security lighting of the yard also is conducive to good RF coverage of the container sorting yard.

With RF antennas placed at each end of the container near the top edge as given in a Container Node requirement, the highest container in a stack will typically have a clear LOS path to at least one light pole mounted AP.

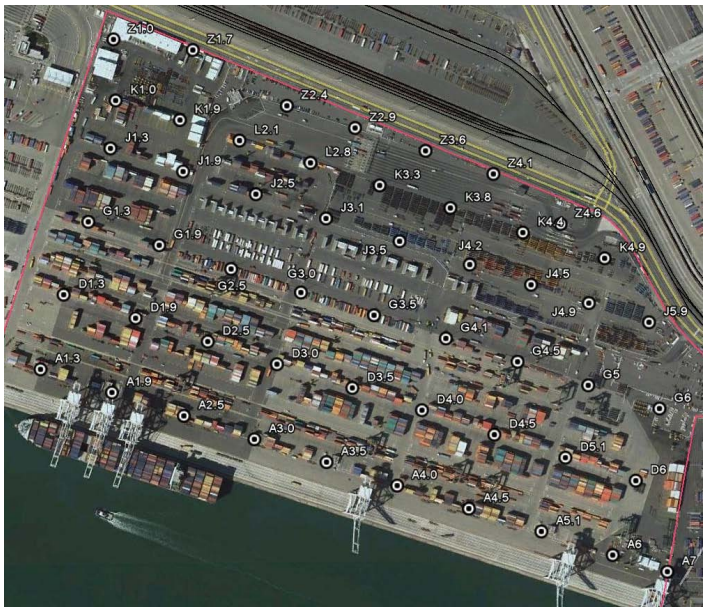

Figure 8 Oakland International Container Terminal light pole locations

As shown in Figure 8, many sorting yards have a matrix of light poles that cover the sorting yard. This light pole pattern is common in North America and Europe. For the Oakland International Container Terminal, the light poles are in a nearly square grid pattern with approximately 120 meters between adjacent light poles. This light pole pattern is ideal for Access Point RF coverage of the containers.

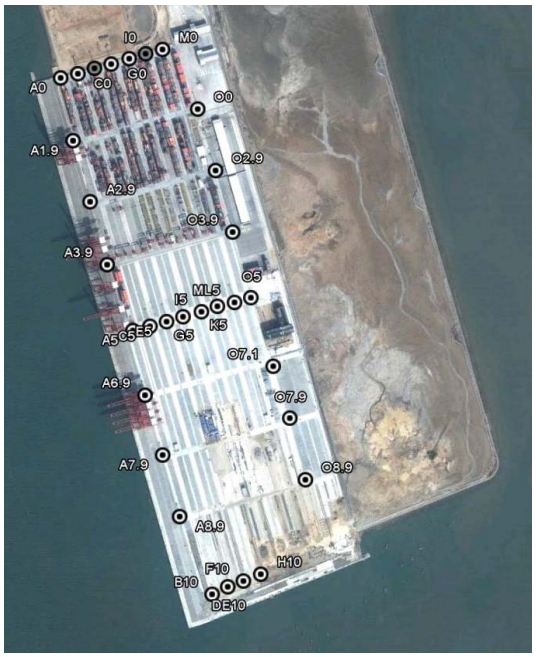

Figure 9 Da Chan Bay Terminal rectangle boundary light pole pattern

A light pole pattern that is common in Asia is shown in Figure 9. For these sorting yards the light poles are concentrated at the ends of aisles on the periphery of the yard. With this light pole pattern containers in the interior of the yard are farther from the Access

Points and more difficult to reach through an RF connection. For these yards more Access Point locations may be required or the use of Wireless Message Relays may be needed.

R-2.1.3.3.3 Access Points shall have the same Tamper Reporting requirements as Container Nodes.

Since criminals may try to block Container Node Alarm messages by disabling an Access Point, Access Points must Alarm if tampering is detected.

R-2.1.3.3.4 Access Points using On-Demand communications with its Shipper NOC shall have the responsibility of detecting missing Container Node Status Reports. A missing Status Report shall result in an immediate Alarm to the NOC.

Some Access Points will not have continuous connectivity with their NOCs. An example is using Satellite Dialup communication only when there is a message to send. Using On-Demand communications can reduce communication costs in some instances.

Access Points expect a Status Report from each Container Node assigned to its portion of the network every X seconds where each node has its own X value depending on Security Mode and remaining stored power.

If an Access Point fails to detect a Status Report from a node within X seconds of its last Status Report, the Access Point shall establish communication with its NOC and send an Alarm message to the NOC containing the following:

- Last Status Report of the missing container Node.
- Time of Missing determination.

R-2.1.3.3.5 Access Points shall report missing Wireless Message Relays with the same requirements of reporting missing Container Nodes.

The Access Point knows the topology of the Container Nodes and Wireless Message Relays. It will not expect Status Reports from Container Nodes that are linked to a missing Wireless Message Relay.

R-2.1.3.3.6 Mobile Access Points shall have GPS. Mobile Access Points shall report their GPS position when queried by their NOC.

Since not all Container Nodes shall have GPS and GPS is not usable for containers buried within a sorting yard stack, the next best container location mechanism is for the Access Point that Container Node is using to provide GPS data. The Access Point GPS gives a general location for the Container Nodes in its network if no other location mechanism is available.

2.1.3.4 Wireless Message Relays

Wireless Message Relays are primarily needed in the train transport scenario. In a mixed CTSN environment on a train (where there are numerous containers that are not CTSN capable) there may be many car lengths between CTSN compliant containers thus

making message Container Node hopping improbable. Wireless Message Relays are either temporarily placed on rail cars in the CTSN gap or the Wireless Message Relays are a permanent component of rail well cars to relay CTSN messages.

Temporary Wireless Message Relays may also be beneficial in sorting yards where Access Point coverage may be insufficient.

Wireless Message Relays may be implemented as specialized Container Node hardware since the Wireless Message Relays Requirements are largely a subset of the Container Node requirements.

R-2.1.3.4.1 Wireless Message Relays, when available, shall be configured by the Shipper's NOC to relay messages between Container Nodes, other Wireless Message Relays and Access Points.

The purpose of the relay is to extend the message routing range between Container Nodes and Access Points. It does this by repeating and routing messages.

R-2.1.3.4.2 Wireless Message Relays shall have the same Tamper reporting requirements as Container Nodes and Access Points.

Disabling or tampering with a WMR is a potential method of preventing a Container Node intrusion Alarm. Some attempts to disable a Wireless Message Relay can be detected before the Relay is successfully disabled. Attempts to disable the Relay are immediately reported as a Tamper Alarm.

R-2.1.3.4.3 Wireless Message Relays are required to have an external power source. The external power source may be intermittent.

This requirement is to accommodate Wireless Message Relays on railroad container well cars where the WMR is powered by a well car wheel or axle mounted generator. The WMR may also be powered by solar power or some other intermittent power source that is not an energy storage device.

R-2.1.3.4.4 Wireless Message Relays with an intermittent external power source shall have an energy storage device for backup power source.

In order to continuously power a Wireless Message Relay a backup power source that has energy storage is needed. This is generally a battery. The capacity of the energy storage must be sufficient to keep the WMR powered for 99.XXXX percent of anticipated intervals of no power from the intermittent power source. The XXXX value must be determined by a study.

R-2.1.3.4.5 The Wireless Message Relay must charge the backup power source from the intermittent external power source when excess power is available.

With this requirement it is possible that a WMR will not require any battery maintenance for many years until the battery materials fail. There is no need for the frequent battery

replacement that are required for non-rechargeable batteries used in many current wireless sensing applications.

R-2.1.3.4.6 A Wireless Message Relay has the same Status Reporting requirements as a Container Node.

Wireless Message Relays may incur the same failures and tampering as Container Nodes therefore a Shipper must know when they are missing due to a failure to receive a Status Report when one is expected.

2.2 Container Requirements

This section contains requirements for CTSN compliant containers.

R-2.2.1.1.1 CTSN containers may be manufactured with integrated CTSN hardware or may be retrofitted.

Retrofitting containers poses issues with routing and protecting wires within the container for power and communications that are not resolved within these requirements.

R-2.2.1.1.2 A CTSN compliant container shall be fitted with the following:

- Sensor Node
- RF Antennas
- Magnetic field Communication and Power Coupler (MCPC).
- Intrusion Sensors
- Optional additional sensors.

R-2.2.1.1.3 A Container Node shall consists of:

- Microcontroller
- Internal backup power
- Power converter for optional external power
- RF Modulator/Demodulator – The modulator/demodulator may be integrated with the antennas instead of the Container Node.
- Magnetic field Coupling Modulator/Demodulator – The modulator/demodulator may be integrated with the CMF coil.
- Passive Sensor monitoring
    - A minimum of enough open/close lines for each container door.
- Optional Sensor Wire Bus for Active sensors – A study is required to determine a suitable low power communication bus for active sensors.
- Optional Sensor Wireless connectivity for cargo/pallet mounted sensors. The requirements of cargo/pallet sensor communications with the Sensor Node are not covered within these requirements.

2.2.2 Container Node Operation Requirements

This section contains requirements related to CTSN Container Node behavior.

R-2.2.2.1.1 The Container Node shall utilize the following categories of sensor and Node events.

- Intrusion – Intrusion can be any of the following but is not limited to these events:
    - Container door opening
    - Unexpected natural or artificial light in container
    - Detection of movement within container
    - Carbon dioxide above normal levels within container (possible human presence).
- Tampering – Tampering can be any of the following but is not limited to these events:
    - Light within the Node's Electronic enclosure.
    - Light within any active sensor's enclosure
    - An increase in the VSWR of the RF transmissions
    - Unexpected power supply voltage fluctuations
    - Unexpected change in sensor electrical current draw
- Electronics Health – An Electronics Health event can be any of the following but is not limited to these events.
    - Backup power supply is near depletion.
    - Failure of active sensor to respond to message from Node
- Safety
    - Sensors indicate smoke, fire or excessive high temperature
    - Sensors indicate chemical leak
- Sensor/Node State
    - Low voltage from external power
    - Switching to internal power
    - Switching to external power (include type of power: solar, kinetic, thermal)

The category of the event is used to determine which personnel to notify.

R-2.2.2.1.2 The Container Node shall utilize the following Attention Level for reporting events:

- **Alarm** – The container node sensor event must be investigated immediately. Notification of responsible personnel must be by the most immediate means.
- **Warning** – The event may indicate a current or future problem and should be investigated but it is not an emergency.
- **Information** – The event is noteworthy and should be reported to the appropriate personnel by non intrusive means. The event by itself does not indicate a problem to investigate.

Each event message to the Container Node's current Shipper Custodian's NOC shall contain an indicator of the severity of the event. The NOC uses the severity of the event to determine what method to use to alert the appropriate Shipper's or emergency response personnel of the event.

R-2.2.2.1.3 Individual CTSN containers shall have the following security modes:

- **Secure** – The Secure Security Mode is used when the container is loaded with cargo and has been sealed.

    - In the Secure Security Mode the following categories of events are Alarm Attention Level:
        - Intrusion
        - Tampering
        - Safety
        - Electronics Heath – Readings of problems with electronics heath could be due to tampering.
- **Unsecure** – The Unsecure Security Mode is utilized when the container is being loaded, unloaded or the cargo is being inspected.
    - The following event categories are expected in the Unsecure Security Mode and are reported as Information Attention Level instead of Alarm or Warning Attention Level:
        - Intrusion
    - The following event categories are reported as Alarm Attention Level:
        - Tampering – No tampering of the container or electronics is allowed
        - Safety – During loading, unloading, or inspection the cargo may be damaged leading to a dangerous heath issue that may not be noticed by the personnel involved.
        - Electronics Health
    - All other Event Categories are Information Attention Level.
- **Inactive** – The Inactive Security Mode is used when the container has no cargo.
    - In this Security Mode the following events are Alarm Attention Level:
        - Tampering
    - In this mode the following events are Warning Attention Level
        - Electronics Health
    - All other Event Categories are Information Attention Level.
- **Maintenance** – In this security mode it is expected that the electronics are undergoing maintenance. No events are reported.

R-2.2.2.1.4 A Container Node shall send a Status Report to its current Shipper Custodian every X seconds.

The purpose of the periodic Status Report is to allow the container's current Shipper Custodian to determine that there may be a security or maintenance problem with a CTSN container if there is a missing Status Report. A Status Report is missing if the Access Point or NOC does not receive a Status Report from a Container Node within a window Y seconds long centered X seconds from the last received Status Report from the Container Node.

A study must be performed to determine a values for X and Y that keeps battery power usage low but has high enough frequency to allow the Shipper Custodian to determine that a node is missing with sufficient time to raise an alarm and get responders to the last known node location so that cargo loss may be minimized.

The value of X may change based on the node's current Security Mode. A Secure Security Mode would require more frequent Status Reports than Inactive Security Mode.

The status report contains the following:

- Current Security Mode
- Power status (remaining hours of stored power)
- Last Alarm event.
- GPS location if available.

R-2.2.2.1.5 All Container Node events are stored into the Node's non-volatile memory with an event timestamp and all information associated with the event. In the case that the non-volatile memory has been filled, new Information and Warning Attention level messages shall be dropped. The last 10 Alarm Attention level messages shall always be kept in non-volatile memory.

This requirement is intended to prevent an intruder from causing Information or Warning category events to fill up the log memory and then break into the container without the Alarm event being logged due to the full log memory. Information or Warning events that would fill the log memory might be caused by pounding on the side of a container that has an acoustic sensor but the processed sound does not indicate an Alarm to the sensor, just a Warning or Information event.

When all but the last 10 entries in a log memory are full all Warning and Info category events are no longer logged but are still reported to the NOC.

R-2.2.2.1.6 A container's CTSN Node shall retain in non-volatile memory the Shipper ID of the Shipper that has CTSN custody of the container. This shall be named the Custody ID.

R-2.2.2.1.7 The Custody ID in the container Node may only be changed by the TDE through the Custodian Shipper's NOC and Container Node network.

This is used to change the Custody Id of a Node to the next shipper to take custody of container when the container changes Shippers.

The authenticity of the message is verified by the digital signature in the message.

R-2.2.2.1.8 A Container Node's Security Mode shall only be changed by the TDE through the Custodian Shipper's NOC and Container Node network.

The authenticity of the message is verified by the digital signature in the message.

R-2.2.2.1.9 An authorized Customs Agent may request that the TDE change a Container Node's Security Mode from Secure to Unsecure or Unsecure to Secure.

The request shall be made to the TDE over the Custom Agency's network to the TDE. See Figure 1.

This requirement is needed for customs officials to inspect containers without causing an Intrusion Alarm.

R-2.2.2.1.10 Node Alarm, Warning and Information event messages shall be reported immediately by the Container Node to the Custodian Shipper's CTSN NOC via the Container Node wireless network.

If the container is not in a container node wireless network when the event occurs, the event message becomes an unreported event message within the node. As soon as the container joins a container node wireless network the node reports all unreported event messages. All Alarm event messages are reported first.

R-2.2.2.1.11 The Container Node shall clear its non-volatile event log upon a Clear Log message from the TDE.

The Container Node shall validate the Clear Log message from the TDE, via the current Custodian Shipper's network, using the TDE's digital signature for the message.

2.2.3 Container Sensor Requirements

This section contains requirements concerning the sensors that are for monitoring container security, integrity, safety and node health. Cargo specific sensors are not covered in this section. Note that security sensing is required while other sensing is optional.

R-2.2.3.1.1 A CTSN Container Node shall detect the occurrence and duration of a container intrusion event.

Container intrusion may be detected using one or more of the following methods:

- **Door open sensor** to detect when a door of the container had been opened. Potential door open sensors are:
  - Mechanical switch
  - Magnetic switch
  - Proximity switch
  - Photo-beam
- **Photo-diode** or similar light sensing device capable of detecting that a door has been opened or an opening has been cut into the container resulting in sun light or exterior artificial light illuminating the interior of the container.
- **Motion sensor** to detect movement in the container where there should be no movement.
- **Carbon dioxide sensor** to detect the presence of persons or animals in the container.

R-2.2.3.1.2 A CTSN container node *may* monitor sensors to detect safety issues.

Sensors to detect safety issues include but are not limited to the following:

- Smoke detection sensor

- Heat sensor
- Chemical detection sensor
- Radiation detection sensor

R-2.2.3.1.3 CTSN container *may* monitor any of the following:

- Environmental parameters inside container
  - Temperature
  - Humidity
  - Acceleration, G-force
- GPS.
- Cargo mounted wireless sensors
  - A study is required to determine a good physical layer and protocol for communicating with Cargo Sensors. One candidate would be Dash-7.

R-2.2.3.1.4 CTSN Container's sensors shall operate at temperatures between -20C and +70C.

Containers are shipped to cold climates such as Alaska, United States and hot climates such as Dubai, UAE.

2.2.4 Container Power Requirements

Power management is one of the most important aspects of any mobile sensing device that also uses RF communication. This section covers power requirements of Container Nodes.

R-2.2.4.1.1 Containers *may* obtain power from self generated means including but not limited to:

- Solar cells
- Kinetic motion

R-2.2.4.1.2 Vehicles and vessels transporting containers and sorting yards *may* provide power to the top or bottom container in a stack via the Coupled Magnetic Field power device.

An example would be a railroad container well car using a permanent magnet on a car wheel or axle with a pickup coil that generates power that is then delivered, via power cable, to a coupled magnetic field power delivery pad on the bottom of the well car directly under the bottom container's Coupled Magnetic Field power coupler.

R-2.2.4.1.3 Vertically stacked containers shall transfer excess Node power from a container being supplied power (either external or self generated) to other containers in a stack by means of a Coupled Magnetic Field between any two vertically adjacent CTSN containers.

The most likely self generated power source for containers would be solar power. Solar power will not work for containers buried in a stack of containers in a sorting yard but a container at the top of a stack can utilize solar power. This requirement allows a container

with a self generated power source to share excess power with other vertically adjacent containers that can not utilize self generated power.

A container with self generated solar power on the top of a stack could provide power to all other CTSN containers in the stack through the Coupled Magnetic Field devices on the containers provided there are no non-CTSN containers in the stack.

In a sorting yard it is possible to place Coupled Magnetic Field devices in the pavement surface at the location for each container stack to provide external power from the bottom of a stack. The pavement placed Coupled Magnetic Field devices are powered from the sorting yard infrastructure. See Figure 6.

The bottom container in a rail well car may be powered from an axle or wheel mounted generator through a Coupled Magnetic Field device in the bottom of the well car. The bottom container could power the top container through another Coupled Magnetic Field device.

R-2.2.4.1.4 CTSN container Coupled Magnetic Field power couplers shall be placed in a location on the container and housed to prevent damage to the power coupler under normal handling of the container.

It would be best if the couplers were flush with the top/bottom of the container and able to sustain a direct impact with the same resilience as the remainder of the top/bottom of the container.

R-2.2.4.1.5 CTSN container Coupled Magnetic Field power couplers shall be placed in a location on the containers to allow power transfer between a 40 foot and longer container placed on top of two 20’ containers in the rail transport container stack configuration.

External power applied to one 20 foot container shall pass up to the 40 foot container and then down to the other 20 foot container unless both 20 foot containers are directly powered by the rail well car.

A likely location for CMF couples is at both ends on top and bottom for a total of four couplers. This configuration allows a long container to be stacked on two 20 foot containers and have at least 1 coupler pair line up for each container.

R-2.2.4.1.6 CTSN container Coupled Magnetic Field power couplers shall be placed in a standard location on containers. The location shall allow 40 foot and larger containers to be stacked in either end-for-end orientation.

The likely configuration for this requirement is to place couplers at a prescribed distance X that is less than 20 foot from the center of the container.

On 20 foot containers the CMF couples would be placed 20’ – X from the end of the container.

A possible value for X is 10'. This would place one CMF in the middle of the top and bottom of the 20' containers. The 40' and longer containers would have 4 CMF, two on and two on bottom 10' from the center line of the container.

R-2.2.4.1.7 Containers shall provide Node power from rechargeable electrical energy storage when external or self generated power is not available or insufficient.

Container electrical energy storage capacity must be sufficient to power communications with adjacent containers or CTSN Wireless Access Point for 99.9XXX% of the statistical durations that external or self generated power is not available.

A study is needed to determine a reasonable value for XXX.

R-2.2.4.1.8 CTSN container power system shall operate at temperatures between -20C and +70C.

CTSN must be able to operate in extreme cold conditions seen in locations such as Alaska and hot locations such as United Arab Emirates.

R-2.2.4.1.9 When a CTSN container is obtaining external or self generated power, excess power shall be transferred to vertically adjacent CTSN containers through the Coupled Magnetic Field power coupler. Stored electrical power is never transferred to another container.

A container with external or self generated power may be able to power a whole stack of containers.

Stored electrical power is never used to power adjacent containers. This prevents tampering by draining the electrical power of a Container Node through external demand.

R-2.2.4.1.10 All cargo mounted sensors shall provide their own power.

The practical constraints of designing a Container Node capable of supplying power to cargo mounted sensors drive this requirement. However, using magnetic coupled power transfer similar to the method used to transfer power between vertically stacked containers should be considered for powering cargo mounted sensors.

R-2.2.4.1.11 When a container is using stored electrical power for the Node, communication with cargo mounted sensors is limited to reduce the stored power drain.

This requirement will need a solid X kBytes/hour limit once the physical medium, protocol and data rate have been determined for container node–cargo sensor communication.

3 Recommendations

Refrigerated containers should be the first type of containers to have CTSN installed

- These containers are continuously powered for refrigeration (except for brief periods) so power is available for the Container Node.
- These containers are used to transport perishable good, with the client and Custodian Shipper having a vested interest in immediate notification elevated temperatures or failure of the refrigeration system.

Another early adoption candidate for CTSN would be containers carrying goods of very high value (example: PC CPU or GPU chips).

During early adoption a small portion of a sorting yard may be retrofitted with the Access Points where CTSN containers are sorted.

During early adoption a small portion of the yard surface may be retrofitted with the Magnetic Coupled Power and Communication pads in appropriated locations within the indicated container placement grid where CTSN containers are sorted.